**[MS-DTYP]:**

**Windows Data Types**

Intellectual Property Rights Notice for Open Specifications Documentation

* **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
* **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
* **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
* **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](http://go.microsoft.com/fwlink/?LinkId=214445) or the [Microsoft Community Promise](http://go.microsoft.com/fwlink/?LinkId=214448). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
* **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the [Patent Map](https://msdn.microsoft.com/en-us/openspecifications/dn750984).
* **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
* **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights**. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

**Tools**. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

**Support.** For questions and support, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

**Revision Summary**

| Date | Revision History | Revision Class | Comments |
| --- | --- | --- | --- |
| 2/14/2008 | 3.1.2 | Editorial | Changed language and formatting in the technical content. |
| 3/14/2008 | 4.0 | Major | Updated and revised the technical content. |
| 6/20/2008 | 5.0 | Major | Updated and revised the technical content. |
| 7/25/2008 | 6.0 | Major | Updated and revised the technical content. |
| 8/29/2008 | 7.0 | Major | Updated and revised the technical content. |
| 10/24/2008 | 8.0 | Major | Updated and revised the technical content. |
| 12/5/2008 | 9.0 | Major | Updated and revised the technical content. |
| 1/16/2009 | 9.0.1 | Editorial | Changed language and formatting in the technical content. |
| 2/27/2009 | 10.0 | Major | Updated and revised the technical content. |
| 4/10/2009 | 10.1 | Minor | Clarified the meaning of the technical content. |
| 5/22/2009 | 11.0 | Major | Updated and revised the technical content. |
| 7/2/2009 | 11.1 | Minor | Clarified the meaning of the technical content. |
| 8/14/2009 | 11.2 | Minor | Clarified the meaning of the technical content. |
| 9/25/2009 | 12.0 | Major | Updated and revised the technical content. |
| 11/6/2009 | 12.1 | Minor | Clarified the meaning of the technical content. |
| 12/18/2009 | 12.2 | Minor | Clarified the meaning of the technical content. |
| 1/29/2010 | 13.0 | Major | Updated and revised the technical content. |
| 3/12/2010 | 13.1 | Minor | Clarified the meaning of the technical content. |
| 4/23/2010 | 13.2 | Minor | Clarified the meaning of the technical content. |
| 6/4/2010 | 14.0 | Major | Updated and revised the technical content. |
| 7/16/2010 | 15.0 | Major | Updated and revised the technical content. |
| 8/27/2010 | 16.0 | Major | Updated and revised the technical content. |
| 10/8/2010 | 17.0 | Major | Updated and revised the technical content. |
| 11/19/2010 | 18.0 | Major | Updated and revised the technical content. |
| 1/7/2011 | 19.0 | Major | Updated and revised the technical content. |
| 2/11/2011 | 20.0 | Major | Updated and revised the technical content. |
| 3/25/2011 | 21.0 | Major | Updated and revised the technical content. |
| 5/6/2011 | 21.1 | Minor | Clarified the meaning of the technical content. |
| 6/17/2011 | 22.0 | Major | Updated and revised the technical content. |
| 9/23/2011 | 22.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 12/16/2011 | 23.0 | Major | Updated and revised the technical content. |
| 3/30/2012 | 24.0 | Major | Updated and revised the technical content. |
| 7/12/2012 | 24.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 10/25/2012 | 25.0 | Major | Updated and revised the technical content. |
| 1/31/2013 | 25.1 | Minor | Clarified the meaning of the technical content. |
| 8/8/2013 | 26.0 | Major | Updated and revised the technical content. |
| 11/14/2013 | 27.0 | Major | Updated and revised the technical content. |
| 2/13/2014 | 27.1 | Minor | Clarified the meaning of the technical content. |
| 5/15/2014 | 28.0 | Major | Updated and revised the technical content. |
| 6/30/2015 | 29.0 | Major | Significantly changed the technical content. |
| 10/16/2015 | 30.0 | Major | Significantly changed the technical content. |
| 7/14/2016 | 31.0 | Major | Significantly changed the technical content. |
| 6/1/2017 | 32.0 | Major | Significantly changed the technical content. |
| 9/15/2017 | 33.0 | Major | Significantly changed the technical content. |
| 12/1/2017 | 34.0 | Major | Significantly changed the technical content. |

Table of Contents

[1 Introduction 8](#_Toc499828890)

[1.1 Glossary 8](#_Toc499828891)

[1.2 References 11](#_Toc499828892)

[1.2.1 Normative References 11](#_Toc499828893)

[1.2.2 Informative References 12](#_Toc499828894)

[1.3 Overview 12](#_Toc499828895)

[1.4 Relationship to Protocols and Other Structures 13](#_Toc499828896)

[1.5 Applicability Statement 13](#_Toc499828897)

[1.6 Versioning and Localization 13](#_Toc499828898)

[1.7 Vendor-Extensible Fields 13](#_Toc499828899)

[2 Data Types 14](#_Toc499828900)

[2.1 Common Base Types 14](#_Toc499828901)

[2.1.1 bit 14](#_Toc499828902)

[2.1.2 byte 14](#_Toc499828903)

[2.1.3 handle\_t 15](#_Toc499828904)

[2.1.4 Integer Types 15](#_Toc499828905)

[2.1.4.1 \_\_int8 15](#_Toc499828906)

[2.1.4.2 \_\_int16 15](#_Toc499828907)

[2.1.4.3 \_\_int32 15](#_Toc499828908)

[2.1.4.4 \_\_int64 15](#_Toc499828909)

[2.1.4.5 hyper 15](#_Toc499828910)

[2.1.5 octet 15](#_Toc499828911)

[2.1.6 wchar\_t 16](#_Toc499828912)

[2.2 Common Data Types 16](#_Toc499828913)

[2.2.1 \_\_int3264 16](#_Toc499828914)

[2.2.2 ADCONNECTION\_HANDLE 16](#_Toc499828915)

[2.2.3 BOOL 16](#_Toc499828916)

[2.2.4 BOOLEAN 16](#_Toc499828917)

[2.2.5 BSTR 17](#_Toc499828918)

[2.2.6 BYTE 17](#_Toc499828919)

[2.2.7 CHAR 17](#_Toc499828920)

[2.2.8 DOUBLE 17](#_Toc499828921)

[2.2.9 DWORD 17](#_Toc499828922)

[2.2.10 DWORD\_PTR 18](#_Toc499828923)

[2.2.11 DWORD32 18](#_Toc499828924)

[2.2.12 DWORD64 18](#_Toc499828925)

[2.2.13 DWORDLONG 18](#_Toc499828926)

[2.2.14 error\_status\_t 18](#_Toc499828927)

[2.2.15 FLOAT 18](#_Toc499828928)

[2.2.16 HANDLE 19](#_Toc499828929)

[2.2.17 HCALL 19](#_Toc499828930)

[2.2.18 HRESULT 19](#_Toc499828931)

[2.2.19 INT 19](#_Toc499828932)

[2.2.20 INT8 19](#_Toc499828933)

[2.2.21 INT16 20](#_Toc499828934)

[2.2.22 INT32 20](#_Toc499828935)

[2.2.23 INT64 20](#_Toc499828936)

[2.2.24 LDAP\_UDP\_HANDLE 20](#_Toc499828937)

[2.2.25 LMCSTR 20](#_Toc499828938)

[2.2.26 LMSTR 20](#_Toc499828939)

[2.2.27 LONG 21](#_Toc499828940)

[2.2.28 LONGLONG 21](#_Toc499828941)

[2.2.29 LONG\_PTR 21](#_Toc499828942)

[2.2.30 LONG32 21](#_Toc499828943)

[2.2.31 LONG64 21](#_Toc499828944)

[2.2.32 LPCSTR 22](#_Toc499828945)

[2.2.33 LPCVOID 22](#_Toc499828946)

[2.2.34 LPCWSTR 22](#_Toc499828947)

[2.2.35 LPSTR 22](#_Toc499828948)

[2.2.36 LPWSTR 22](#_Toc499828949)

[2.2.37 NET\_API\_STATUS 23](#_Toc499828950)

[2.2.38 NTSTATUS 23](#_Toc499828951)

[2.2.39 PCONTEXT\_HANDLE 23](#_Toc499828952)

[2.2.40 QWORD 23](#_Toc499828953)

[2.2.41 RPC\_BINDING\_HANDLE 24](#_Toc499828954)

[2.2.42 SHORT 24](#_Toc499828955)

[2.2.43 SIZE\_T 24](#_Toc499828956)

[2.2.44 STRING 24](#_Toc499828957)

[2.2.45 UCHAR 25](#_Toc499828958)

[2.2.46 UINT 25](#_Toc499828959)

[2.2.47 UINT8 25](#_Toc499828960)

[2.2.48 UINT16 25](#_Toc499828961)

[2.2.49 UINT32 25](#_Toc499828962)

[2.2.50 UINT64 25](#_Toc499828963)

[2.2.51 ULONG 26](#_Toc499828964)

[2.2.52 ULONG\_PTR 26](#_Toc499828965)

[2.2.53 ULONG32 26](#_Toc499828966)

[2.2.54 ULONG64 26](#_Toc499828967)

[2.2.55 ULONGLONG 26](#_Toc499828968)

[2.2.56 UNICODE 26](#_Toc499828969)

[2.2.57 UNC 27](#_Toc499828970)

[2.2.58 USHORT 28](#_Toc499828971)

[2.2.59 VOID 28](#_Toc499828972)

[2.2.60 WCHAR 28](#_Toc499828973)

[2.2.61 WORD 28](#_Toc499828974)

[2.3 Common Data Structures 28](#_Toc499828975)

[2.3.1 EVENT\_DESCRIPTOR 28](#_Toc499828976)

[2.3.2 EVENT\_HEADER 29](#_Toc499828977)

[2.3.3 FILETIME 31](#_Toc499828978)

[2.3.4 GUID and UUID 31](#_Toc499828979)

[2.3.4.1 GUID--RPC IDL representation 31](#_Toc499828980)

[2.3.4.2 GUID--Packet Representation 32](#_Toc499828981)

[2.3.4.3 GUID--Curly Braced String Representation 32](#_Toc499828982)

[2.3.5 LARGE\_INTEGER 32](#_Toc499828983)

[2.3.6 LCID 33](#_Toc499828984)

[2.3.7 LUID 33](#_Toc499828985)

[2.3.8 MULTI\_SZ 33](#_Toc499828986)

[2.3.9 OBJECT\_TYPE\_LIST 33](#_Toc499828987)

[2.3.10 RPC\_UNICODE\_STRING 34](#_Toc499828988)

[2.3.11 SERVER\_INFO\_100 34](#_Toc499828989)

[2.3.12 SERVER\_INFO\_101 35](#_Toc499828990)

[2.3.13 SYSTEMTIME 38](#_Toc499828991)

[2.3.14 UINT128 38](#_Toc499828992)

[2.3.15 ULARGE\_INTEGER 38](#_Toc499828993)

[2.4 Constructed Security Types 38](#_Toc499828994)

[2.4.1 SID\_IDENTIFIER\_AUTHORITY 38](#_Toc499828995)

[2.4.1.1 RPC\_SID\_IDENTIFIER\_AUTHORITY 39](#_Toc499828996)

[2.4.2 SID 40](#_Toc499828997)

[2.4.2.1 SID String Format Syntax 40](#_Toc499828998)

[2.4.2.2 SID--Packet Representation 41](#_Toc499828999)

[2.4.2.3 RPC\_SID 41](#_Toc499829000)

[2.4.2.4 Well-Known SID Structures 42](#_Toc499829001)

[2.4.3 ACCESS\_MASK 50](#_Toc499829002)

[2.4.4 ACE 53](#_Toc499829003)

[2.4.4.1 ACE\_HEADER 53](#_Toc499829004)

[2.4.4.1.1 ACE\_HEADER--RPC representation 55](#_Toc499829005)

[2.4.4.2 ACCESS\_ALLOWED\_ACE 55](#_Toc499829006)

[2.4.4.3 ACCESS\_ALLOWED\_OBJECT\_ACE 56](#_Toc499829007)

[2.4.4.4 ACCESS\_DENIED\_ACE 58](#_Toc499829008)

[2.4.4.5 ACCESS\_DENIED\_OBJECT\_ACE 58](#_Toc499829009)

[2.4.4.6 ACCESS\_ALLOWED\_CALLBACK\_ACE 60](#_Toc499829010)

[2.4.4.7 ACCESS\_DENIED\_CALLBACK\_ACE 60](#_Toc499829011)

[2.4.4.8 ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE 61](#_Toc499829012)

[2.4.4.9 ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE 62](#_Toc499829013)

[2.4.4.10 SYSTEM\_AUDIT\_ACE 64](#_Toc499829014)

[2.4.4.11 SYSTEM\_AUDIT\_OBJECT\_ACE 65](#_Toc499829015)

[2.4.4.12 SYSTEM\_AUDIT\_CALLBACK\_ACE 66](#_Toc499829016)

[2.4.4.13 SYSTEM\_MANDATORY\_LABEL\_ACE 67](#_Toc499829017)

[2.4.4.13.1 SYSTEM\_MANDATORY\_LABEL\_ACE--RPC Representation 68](#_Toc499829018)

[2.4.4.14 SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE 68](#_Toc499829019)

[2.4.4.15 SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE 70](#_Toc499829020)

[2.4.4.16 SYSTEM\_SCOPED\_POLICY\_ID\_ACE 71](#_Toc499829021)

[2.4.4.17 Conditional ACEs 71](#_Toc499829022)

[2.4.4.17.1 Conditional ACE Expressions 71](#_Toc499829023)

[2.4.4.17.2 Security Attributes 72](#_Toc499829024)

[2.4.4.17.3 Conditional ACE Applicability 72](#_Toc499829025)

[2.4.4.17.4 Conditional ACE Binary Formats 72](#_Toc499829026)

[2.4.4.17.5 Literal Tokens 73](#_Toc499829027)

[2.4.4.17.6 Relational Operator Tokens 74](#_Toc499829028)

[2.4.4.17.7 Logical Operator Tokens 76](#_Toc499829029)

[2.4.4.17.8 Attribute Tokens 78](#_Toc499829030)

[2.4.4.17.9 Examples: Conditional Expression Binary Representation 78](#_Toc499829031)

[2.4.5 ACL 81](#_Toc499829032)

[2.4.5.1 ACL--RPC Representation 83](#_Toc499829033)

[2.4.6 SECURITY\_DESCRIPTOR 83](#_Toc499829034)

[2.4.6.1 SECURITY\_DESCRIPTOR--RPC Representation 86](#_Toc499829035)

[2.4.7 SECURITY\_INFORMATION 86](#_Toc499829036)

[2.4.8 TOKEN\_MANDATORY\_POLICY 87](#_Toc499829037)

[2.4.9 MANDATORY\_INFORMATION 88](#_Toc499829038)

[2.4.10 CLAIM\_SECURITY\_ATTRIBUTE 88](#_Toc499829039)

[2.4.10.1 CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 88](#_Toc499829040)

[2.4.10.2 CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE 90](#_Toc499829041)

[2.5 Additional Information for Security Types 91](#_Toc499829042)

[2.5.1 Security Descriptor Description Language 91](#_Toc499829043)

[2.5.1.1 Syntax 91](#_Toc499829044)

[2.5.1.2 Security Attribute Names 99](#_Toc499829045)

[2.5.1.2.1 Simple Attribute Name Form 99](#_Toc499829046)

[2.5.1.2.2 @Prefixed Attribute Name Form 99](#_Toc499829047)

[2.5.1.3 Parentheses and Order of Precedence 99](#_Toc499829048)

[2.5.1.4 SDDL String to Binary Security Descriptor Examples 100](#_Toc499829049)

[2.5.2 Token/Authorization Context 103](#_Toc499829050)

[2.5.2.1 Token/Authorization Context Algorithms 104](#_Toc499829051)

[2.5.2.1.1 GatherGroupMembershipForSystem 104](#_Toc499829052)

[2.5.2.1.2 AddPrivilegesToToken 105](#_Toc499829053)

[2.5.3 Security Descriptor Algorithms 105](#_Toc499829054)

[2.5.3.1 Support Functions 106](#_Toc499829055)

[2.5.3.1.1 SidInToken 106](#_Toc499829056)

[2.5.3.1.2 SidDominates 106](#_Toc499829057)

[2.5.3.1.3 GetScopedPolicySid 107](#_Toc499829058)

[2.5.3.1.4 GetCentralizedAccessPolicy 107](#_Toc499829059)

[2.5.3.1.5 EvaluateAceCondition 108](#_Toc499829060)

[2.5.3.1.6 LookupAttributeInToken 111](#_Toc499829061)

[2.5.3.1.7 LookupAttributeInSacl 112](#_Toc499829062)

[2.5.3.1.8 PushStackOperand 112](#_Toc499829063)

[2.5.3.1.9 PushStackResult 113](#_Toc499829064)

[2.5.3.1.10 PopStack 113](#_Toc499829065)

[2.5.3.2 Access Check Algorithm Pseudocode 113](#_Toc499829066)

[2.5.3.3 MandatoryIntegrityCheck Algorithm Pseudocode 120](#_Toc499829067)

[2.5.3.3.1 FindAceByType 122](#_Toc499829068)

[2.5.3.4 Algorithm for Creating a Security Descriptor 122](#_Toc499829069)

[2.5.3.4.1 CreateSecurityDescriptor 123](#_Toc499829070)

[2.5.3.4.2 ComputeACL 125](#_Toc499829071)

[2.5.3.4.3 ContainsInheritableACEs 128](#_Toc499829072)

[2.5.3.4.4 ComputeInheritedACLfromParent 128](#_Toc499829073)

[2.5.3.4.5 ComputeInheritedACLfromCreator 130](#_Toc499829074)

[2.5.3.4.6 PreProcessACLfromCreator 131](#_Toc499829075)

[2.5.3.4.7 PostProcessACL 132](#_Toc499829076)

[2.6 ServerGetInfo Abstract Interface 133](#_Toc499829077)

[2.7 Impersonation Abstract Interfaces 134](#_Toc499829078)

[2.7.1 StartImpersonation 134](#_Toc499829079)

[2.7.2 EndImpersonation 135](#_Toc499829080)

[2.7.3 GetAccessToken 135](#_Toc499829081)

[3 Structure Examples 136](#_Toc499829082)

[4 Security Considerations 137](#_Toc499829083)

[5 Appendix A: Full MS-DTYP IDL 138](#_Toc499829084)

[6 Appendix B: Product Behavior 143](#_Toc499829085)

[7 Change Tracking 149](#_Toc499829086)

[8 Index 150](#_Toc499829087)

# Introduction

This document provides a collection of commonly used data types, which are categorized into two basic types: common base types and common data types. The common base types are those types that Microsoft compilers natively support. The common data types are data types that are frequently used by many protocols. These data types are user-defined types.

## Glossary

This document uses the following terms:

**Active Directory**: A general-purpose network directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) also refers to the Windows implementation of a directory service. [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) stores information about a variety of objects in the network. User accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) describes both forms. For more information, see [[MS-AUTHSOD]](%5bMS-AUTHSOD%5d.pdf#Section_953d700a57cb4cf7b0c3a64f34581cc9) section 1.1.1.5.2, Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Kerberos, and DNS.

**American National Standards Institute (ANSI) character set**: A character set defined by a code page approved by the American National Standards Institute (ANSI). The term "ANSI" as used to signify Windows code pages is a historical reference and a misnomer that persists in the Windows community. The source of this misnomer stems from the fact that the Windows code page 1252 was originally based on an ANSI draft, which became International Organization for Standardization (ISO) Standard 8859-1 [[ISO/IEC-8859-1]](https://go.microsoft.com/fwlink/?LinkId=90689). In Windows, the ANSI character set can be any of the following code pages: 1252, 1250, 1251, 1253, 1254, 1255, 1256, 1257, 1258, 874, 932, 936, 949, or 950. For example, "ANSI application" is usually a reference to a non-[**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) or code-page-based application. Therefore, "ANSI character set" is often misused to refer to one of the character sets defined by a Windows code page that can be used as an active system code page; for example, character sets defined by code page 1252 or character sets defined by code page 950. Windows is now based on [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8), so the use of ANSI character sets is strongly discouraged unless they are used to interoperate with legacy applications or legacy data.

**big-endian**: Multiple-byte values that are byte-ordered with the most significant byte stored in the memory location with the lowest address.

**binary large object (BLOB)**: A discrete packet of data that is stored in a database and is treated as a sequence of uninterpreted bytes.

**Component Object Model (COM)**: An object-oriented programming model that defines how objects interact within a single process or between processes. In [**COM**](#gt_ef2ebebc-1760-407a-9ace-af48f9050e02), clients have access to an object through interfaces implemented on the object. For more information, see [[MS-DCOM]](%5bMS-DCOM%5d.pdf#Section_4a893f3dbd2948cd9f43d9777a4415b0).

**curly braced GUID string**: The string representation of a 128-bit globally unique identifier ([**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1)) using the form {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}, where X denotes a hexadecimal digit. The string representation between the enclosing braces is the standard representation of a GUID as described in [[RFC4122]](https://go.microsoft.com/fwlink/?LinkId=90460) section 3. Unlike a GUIDString, a curly braced GUID string includes enclosing braces.

**discretionary access control list (DACL)**: An access control list (ACL) that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.

**Distributed File System (DFS)**: A file system that logically groups physical shared folders located on different servers by transparently connecting them to one or more hierarchical namespaces. [**DFS**](#gt_0b8086c9-d025-45b8-bf09-6b5eca72713e) also provides fault-tolerance and load-sharing capabilities.

**domain**: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a domain controller (DC) and host a member list that identifies all members of the domain, as well as optionally hosting the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

**fully qualified domain name (FQDN)**: An unambiguous domain name that gives an absolute location in the Domain Name System's (DNS) hierarchy tree, as defined in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) section 3.1 and [[RFC2181]](https://go.microsoft.com/fwlink/?LinkId=127732) section 11.

**globally unique identifier (GUID)**: A term used interchangeably with [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) must be used for generating the [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). See also [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3).

**handle**: Any token that can be used to identify and access an object such as a device, file, or a window.

**Interface Definition Language (IDL)**: The International Standards Organization (ISO) standard language for specifying the interface for remote procedure calls. For more information, see [C706] section 4.

**Internet host name**: The name of a host as defined in [[RFC1123]](https://go.microsoft.com/fwlink/?LinkId=90268) section 2.1, with the extensions described in [[MS-HNDS]](%5bMS-HNDS%5d.pdf#Section_eff5b201ad32485dbbed1d07ad069d5c).

**little-endian**: Multiple-byte values that are byte-ordered with the least significant byte stored in the memory location with the lowest address.

**marshaling**: The act of formatting COM parameters for transmission over a [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331). For more information, see [MS-DCOM].

**Microsoft Interface Definition Language (MIDL)**: The Microsoft implementation and extension of the OSF-DCE [**Interface Definition Language (IDL)**](#gt_73177eec-4092-420f-92c5-60b2478df824). [**MIDL**](#gt_9c5903c1-1477-4181-b451-3ba1e34a0c0c) can also mean the [**Interface Definition Language (IDL)**](#gt_73177eec-4092-420f-92c5-60b2478df824) compiler provided by Microsoft. For more information, see [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15).

**NetBIOS host name**: The NetBIOS name of a host (as specified in [[RFC1001]](https://go.microsoft.com/fwlink/?LinkId=90260) section 14 and [[RFC1002]](https://go.microsoft.com/fwlink/?LinkId=90261) section 4), with the extensions described in [[MS-NBTE]](%5bMS-NBTE%5d.pdf#Section_3461cfa83d284fa38163131bf1046fa3).

**organization**: A security group that contains additional fields for describing hierarchical relationships between organizations.

**Remote Access Service (RAS) server**: A type of network access server (NAS) that provides modem dial-up or virtual private network (VPN) access to a network.

**remote procedure call (RPC)**: A communication protocol used primarily between client and server. The term has three definitions that are often used interchangeably: a runtime environment providing for communication facilities between computers (the RPC runtime); a set of request-and-response message exchanges between computers (the RPC exchange); and the single message from an RPC exchange (the RPC message). For more information, see [C706].

**resource manager (RM)**: The participant that is responsible for coordinating the state of a resource with the outcome of atomic transactions. For a specified transaction, a resource manager enlists with exactly one transaction manager to vote on that transaction outcome and to obtain the final outcome. A resource manager is either durable or volatile, depending on its resource.

**security identifier (SID)**: An identifier for security principals that is used to identify an account or a group. Conceptually, the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) is composed of an account authority portion (typically a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca)) and a smaller integer representing an identity relative to the account authority, termed the relative identifier (RID). The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) format is specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.2; a string representation of [**SIDs**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) is specified in [MS-DTYP] section 2.4.2 and [[MS-AZOD]](%5bMS-AZOD%5d.pdf#Section_5a0a0a3ec7a742e1b5f2cc8d8bd9739e) section 1.1.1.2.

**share**: A resource offered by a Common Internet File System (CIFS) server for access by CIFS clients over the network. A [**share**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3) typically represents a directory tree and its included files (referred to commonly as a "disk share" or "file share") or a printer (a "print share"). If the information about the [**share**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3) is saved in persistent store (for example, Windows registry) and reloaded when a file server is restarted, then the [**share**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3) is referred to as a "sticky share". Some [**share**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3) names are reserved for specific functions and are referred to as special [**shares**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3): IPC$, reserved for interprocess communication, ADMIN$, reserved for remote administration, and A$, B$, C$ (and other local disk names followed by a dollar sign), assigned to local disk devices.

**system access control list (SACL)**: An access control list (ACL) that controls the generation of audit messages for attempts to access a securable object. The ability to get or set an object's [**SACL**](#gt_c189801e-3752-4715-88f4-17804dad5782) is controlled by a privilege typically held only by system administrators.

**Unicode**: A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) standard [[UNICODE5.0.0/2007]](https://go.microsoft.com/fwlink/?LinkId=154659) provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

**Unicode character**: Unless otherwise specified, a 16-bit UTF-16 code unit.

**Unicode string**: A [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) 8-bit string is an ordered sequence of 8-bit units, a [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) 16-bit string is an ordered sequence of 16-bit code units, and a [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) 32-bit string is an ordered sequence of 32-bit code units. In some cases, it could be acceptable not to terminate with a terminating null character. Unless otherwise specified, all [**Unicode strings**](#gt_b069acb4-e364-453e-ac83-42d469bb339e) follow the UTF-16LE encoding scheme with no Byte Order Mark (BOM).

**universally unique identifier (UUID)**: A 128-bit value. UUIDs can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) objects. UUIDs are highly likely to be unique. UUIDs are also known as [**globally unique identifiers (GUIDs)**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) and these terms are used interchangeably in the Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the UUID. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [C706] must be used for generating the UUID.

**unmarshal**: The process of deserializing one or more data structures from an octet stream using a specific transfer syntax (for example, unmarshaling a 32-bit integer).

**UTF-16**: A standard for encoding [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0), defined in the Unicode standard, in which the most commonly used characters are defined as double-byte characters. Unless specified otherwise, this term refers to the UTF-16 encoding form specified in [UNICODE5.0.0/2007] section 3.9.

**UTF-8**: A byte-oriented standard for encoding [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0), defined in the Unicode standard. Unless specified otherwise, this term refers to the UTF-8 encoding form specified in [UNICODE5.0.0/2007] section 3.9.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [[RFC2119]](https://go.microsoft.com/fwlink/?LinkId=90317). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](https://go.microsoft.com/fwlink/?linkid=850906).

### Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[C706] The Open Group, "DCE 1.1: Remote Procedure Call", C706, August 1997, [https://www2.opengroup.org/ogsys/catalog/c706](https://go.microsoft.com/fwlink/?LinkId=89824)

[IEEE754] IEEE, "IEEE Standard for Binary Floating-Point Arithmetic", IEEE 754-1985, October 1985, [http://ieeexplore.ieee.org/servlet/opac?punumber=2355](https://go.microsoft.com/fwlink/?LinkId=89903)

[IETFDRAFT-PK-FRESH] Moore, S., Miller, P., and Short, M., Ed., "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), Freshness Extension", draft-short-pkinit-freshness-00, October 2014, [https://tools.ietf.org/html/draft-short-pkinit-freshness](https://go.microsoft.com/fwlink/?LinkId=534982)

[ISO/IEC-8859-1] International Organization for Standardization, "Information Technology -- 8-Bit Single-Byte Coded Graphic Character Sets -- Part 1: Latin Alphabet No. 1", ISO/IEC 8859-1, 1998, [http://www.iso.org/iso/home/store/catalogue\_tc/catalogue\_detail.htm?csnumber=28245](https://go.microsoft.com/fwlink/?LinkId=90689)

**Note** There is a charge to download the specification.

[ISO/IEC-9899] International Organization for Standardization, "Programming Languages - C", ISO/IEC 9899:TC2, May 2005, [http://www.open-std.org/jtc1/sc22/wg14/www/docs/n1124.pdf](https://go.microsoft.com/fwlink/?LinkId=89921)

[MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a)".

[MS-APDS] Microsoft Corporation, "[Authentication Protocol Domain Support](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e)".

[MS-ERREF] Microsoft Corporation, "[Windows Error Codes](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90)".

[MS-GPCAP] Microsoft Corporation, "[Group Policy: Central Access Policies Protocol Extension](%5bMS-GPCAP%5d.pdf#Section_5189d5c912c2491cbf16f7008c46c6fb)".

[MS-KILE] Microsoft Corporation, "[Kerberos Protocol Extensions](%5bMS-KILE%5d.pdf#Section_2a32282edd484ad9a542609804b02cc9)".

[MS-LCID] Microsoft Corporation, "[Windows Language Code Identifier (LCID) Reference](%5bMS-LCID%5d.pdf#Section_70feba9f294e491eb6eb56532684c37f)".

[MS-NBTE] Microsoft Corporation, "[NetBIOS over TCP (NBT) Extensions](%5bMS-NBTE%5d.pdf#Section_3461cfa83d284fa38163131bf1046fa3)".

[MS-NLMP] Microsoft Corporation, "[NT LAN Manager (NTLM) Authentication Protocol](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)".

[MS-PAC] Microsoft Corporation, "[Privilege Attribute Certificate Data Structure](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962)".

[MS-RPCE] Microsoft Corporation, "[Remote Procedure Call Protocol Extensions](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15)".

[MS-SFU] Microsoft Corporation, "[Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol](%5bMS-SFU%5d.pdf#Section_3bff58648135400ebdd933b552051d94)".

[MS-SMB2] Microsoft Corporation, "[Server Message Block (SMB) Protocol Versions 2 and 3](%5bMS-SMB2%5d.pdf#Section_5606ad475ee0437a817e70c366052962)".

[MS-TLSP] Microsoft Corporation, "[Transport Layer Security (TLS) Profile](%5bMS-TLSP%5d.pdf#Section_58aba05b62b04cd1b88bdc8a24920346)".

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987, [http://www.ietf.org/rfc/rfc1035.txt](https://go.microsoft.com/fwlink/?LinkId=90264)

[RFC1123] Braden, R., "Requirements for Internet Hosts - Application and Support", RFC 1123, October 1989, [http://www.ietf.org/rfc/rfc1123.txt](https://go.microsoft.com/fwlink/?LinkId=90268)

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, [http://www.rfc-editor.org/rfc/rfc2119.txt](https://go.microsoft.com/fwlink/?LinkId=90317)

[RFC3986] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, [http://www.rfc-editor.org/rfc/rfc3986.txt](https://go.microsoft.com/fwlink/?LinkId=90453)

[RFC4122] Leach, P., Mealling, M., and Salz, R., "A Universally Unique Identifier (UUID) URN Namespace", RFC 4122, July 2005, [http://www.rfc-editor.org/rfc/rfc4122.txt](https://go.microsoft.com/fwlink/?LinkId=90460)

[RFC4291] Hinden, R. and Deering, S., "IP Version 6 Addressing Architecture", RFC 4291, February 2006, [http://www.ietf.org/rfc/rfc4291.txt](https://go.microsoft.com/fwlink/?LinkId=90464)

[RFC5234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, [http://www.rfc-editor.org/rfc/rfc5234.txt](https://go.microsoft.com/fwlink/?LinkId=123096)

### Informative References

[DALB] Dalbey, J., "Pseudocode Standard", May 2008, [http://users.csc.calpoly.edu/~jdalbey/SWE/pdl\_std.html](https://go.microsoft.com/fwlink/?LinkId=89842)

[MS-ADOD] Microsoft Corporation, "[Active Directory Protocols Overview](%5bMS-ADOD%5d.pdf#Section_5ff67bf4c14548cb89cd4f5482d94664)".

[MS-SMB] Microsoft Corporation, "[Server Message Block (SMB) Protocol](%5bMS-SMB%5d.pdf#Section_f210069c70864dc2885e861d837df688)".

[MSDN-ACCTOKENS] Microsoft Corporation, "Access Tokens", [http://msdn.microsoft.com/en-us/library/aa374909.aspx](https://go.microsoft.com/fwlink/?LinkId=89949)

[MSDN-AuthzAccessCheck] Microsoft Corporation, "AuthzAccessCheck function", [http://msdn.microsoft.com/en-us/library/aa375788%28v=VS.85%29.aspx](https://go.microsoft.com/fwlink/?LinkId=204597)

[MSDN-SDDLforDevObj] Microsoft Corporation, "SDDL for Device Objects", [http://msdn.microsoft.com/en-us/library/ff563667.aspx](https://go.microsoft.com/fwlink/?LinkId=114214)

[RFC3530] Shepler, S., et al., "Network File System (NFS) version 4 Protocol", RFC 3530, April 2003, [http://www.ietf.org/rfc/rfc3530.txt](https://go.microsoft.com/fwlink/?LinkId=90430)

[Tanenbaum] Tanenbaum, A.S., "Modern Operating Systems", Prentice Hall, 2001, ISBN 0-13-092641-8.

## Overview

Two types of data structures are specified in this document: data structures that are specified in terms of the wire format and data structures that are RPC-marshaled as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15). The latter are specified by using the [**Interface Definition Language (IDL)**](#gt_73177eec-4092-420f-92c5-60b2478df824) that is defined in [MS-RPCE] section 2.2.4.

For some types of data, both formats are shown. For example, both formats are shown if some protocols use the raw wire format but other protocols use the RPC-marshaled format. Any protocol that uses a data structure name in its IDL necessarily implies the use of the IDL version of the data structure. Any other use implies the use of the wire format version unless otherwise specified by the protocol that uses the data structure.

## Relationship to Protocols and Other Structures

The data structures in this document are generic data structures that are used by many protocols.

## Applicability Statement

Not applicable.

## Versioning and Localization

Not applicable.

## Vendor-Extensible Fields

HRESULT: Vendors can choose their own values, as long as the **C** bit (0x20000000) is set, indicating it is a customer code.

NTSTATUS: Vendors can choose their own values for this field, as long as the **C** bit (0x20000000) is set, indicating it is a customer code.

[SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d): Vendors can extend **Sbz1** by setting **RM Control Valid** to 0x1.

# Data Types

The following sections describe data types that include common base types, data types, and data structures.

Many protocols are intended to be extensions of local programming models. Other protocols have a distinct purpose but share many common elements. This section is a discussion of data types that are common to many protocols.

In some cases, a component might not follow the typical practice and where that applies, the relevant specification specifies the actual practice.

Integer names often have an alias, which is interchangeable with the integer name; there is no difference in using either the name or its alias.

## Common Base Types

This section contains commonly used primitive data types.

The use of the [**Interface Definition Language (IDL)**](#gt_73177eec-4092-420f-92c5-60b2478df824) implies RPC marshaling unless custom marshaling is specified.

Unless explicitly noted in this document, any integer, either signed or unsigned, is in memory order before RPC marshalling. It is implementation dependent[<1>](#Appendix_A_1" \o "Product behavior note 1) whether the memory order is [**little-endian**](#gt_079478cb-f4c5-4ce5-b72b-2144da5d2ce7) or [**big-endian**](#gt_6f6f9e8e-5966-4727-8527-7e02fb864e7e).

For packets, the bit numbering convention followed is the same as that used in RFCs, namely: the high (most significant) bit of the first byte to hit the wire is in packet bit 0, and the low bit of the last byte to hit the wire is in packet bit 31 (so that the bits are shown from left-to-right in the order they naturally appear over the network).

Packet byte/bit order

Figure 1: Packet byte/bit order

Unless otherwise specified, the bytes of a multi-byte integer field are assumed to be transmitted in big-endian order, also referred to as Network Byte Order. That is, if the packet shown above represented a 32-bit integer, then Byte 1 would be its high-order byte and Byte 4 its low-order byte. Certain protocols use little-endian order, as specified in the corresponding technical documents; for example, [[MS-SMB2]](%5bMS-SMB2%5d.pdf#Section_5606ad475ee0437a817e70c366052962).

### bit

A bit is a single binary digit, which is the smallest primitive element of any data structure.

### byte

The byte type specifies an 8-bit data item.

A byte is a base [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) type as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 4.2.9.5. A byte item is opaque in that its contents are not interpreted, as a character data type might be.

### handle\_t

The **handle\_t** data type is used to represent an explicit RPC binding handle, as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) and [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2. This data type is a predefined type of the [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) and does not require an explicit declaration.

A primitive binding handle is a data object that can be used by the application to represent the binding. It can appear as a type specifier in typedef declarations, general declarations, and function declarations (as a function-return-type specifier and a parameter-type specifier).

### Integer Types

Microsoft C/C++ supports different sizes of integer types. An 8-bit, 16-bit, 32-bit, or 64-bit integer variable can be declared by using the \_\_int*n* type specifier, where *n* is 8, 16, 32, or 64.

The types [\_\_int8](#Section_d49d02028b2d47c591c8c91351e13b5e), [\_\_int16](#Section_a8d4667982ab481684a0e64c517fd98c), and [\_\_int32](#Section_d7de9ef39db94365aaa57f3e27820f0b) are synonyms for the [**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583)/ISO C types (as specified in [[ISO/IEC-9899]](https://go.microsoft.com/fwlink/?LinkId=89921)) that have the same size. They are useful for writing portable code that behaves identically across multiple platforms.

#### \_\_int8

An 8-bit signed integer (range: –128 to 127 decimal). The first bit, the most significant bit (MSB), is the signing bit. This type can be specified as unsigned by using the unsigned data-type modifier. As an unsigned \_\_int8, the range is from 0 to 255 decimal.

#### \_\_int16

A 16-bit signed integer (range: –32768 to 32767 decimal). The first bit (MSB) is the signing bit.

This type can be specified as unsigned by using the unsigned data-type modifier. As an unsigned \_\_int16, the range is from 0 to 65535 decimal.

#### \_\_int32

A 32-bit signed integer (range: –2147483648 to 2147483647 decimal). The first bit (MSB) is the signing bit.

This type can be specified as unsigned by using the unsigned data-type modifier. As an unsigned \_\_int32, the range is from 0 to 4294967295 decimal.

#### \_\_int64

A 64-bit signed integer (range: –9223372036854775808 to 9223372036854775807 decimal). The first bit (MSB) is the signing bit.

This type can be specified as unsigned by using the unsigned data-type modifier. As an unsigned \_\_int64, the range is from 0 to 18446744073709551615 decimal.

#### hyper

The keyword **hyper** indicates a 64-bit integer that can be declared as either signed or unsigned.

### octet

The octet type specifies an 8-bit data item.

An **octet** is an 8-bit data type as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 14.2.

### wchar\_t

A [**Unicode character**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0) for use with the [**Microsoft Interface Definition Language (MIDL)**](#gt_9c5903c1-1477-4181-b451-3ba1e34a0c0c) compiler.

This type is declared as follows:

1. typedef unsigned short wchar\_t;

## Common Data Types

This section contains simple data types that are defined by either a C/C++ typedef or #define statement. The data types in this section are essentially aliases for C/C++ primitive data types.

### \_\_int3264

An alias that is resolved to either:

* An [\_\_int32](#Section_d7de9ef39db94365aaa57f3e27820f0b) in a 32-bit translation and execution environment, or
* An [\_\_int64](#Section_fb42d70d7efc4b0295615c9747be4a59) in a 64-bit translation and execution environment. For backward compatibility, it is 32-bit on the wire. The higher 4 bytes MUST be truncated on the sender side during [**marshaling**](#gt_e0245240-9927-4991-85af-f5babcd95bfd) and MUST be extended appropriately (signed or unsigned), as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 14.2.5, on the receiving side during [**unmarshaling**](#gt_3805d4b6-fddb-4079-9f39-b70a4945f97d).

### ADCONNECTION\_HANDLE

A handle to an ADConnection object that is used to manage the TCP connections that are used for communication between a client and [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) servers.

This type is declared as follows:

1. typedef void\* ADCONNECTION\_HANDLE;

### BOOL

A BOOL is a 32-bit field that is set to 1 to indicate **TRUE**, or 0 to indicate **FALSE**.

This type is declared as follows:

1. typedef int BOOL, \*PBOOL, \*LPBOOL;

### BOOLEAN

A BOOLEAN is an 8-bit field that is set to 1 to indicate **TRUE**, or 0 to indicate **FALSE**.

This type is declared as follows:

1. typedef BYTE BOOLEAN, \*PBOOLEAN;

### BSTR

A BSTR is a pointer to a null-terminated character string in which the string length is stored with the string. This type is declared as follows:

1. typedef WCHAR\* BSTR;

Because the length is stored with the string, BSTR variables can contain embedded null characters. For example:

1. [4 bytes (length prefix)],
2. wchar\_t[length], [\0]

### BYTE

A BYTE is an 8-bit unsigned value that corresponds to a single [octet](#Section_a3bd8ab11d4044be8c30dddae7183e31) in a network protocol.

This type is declared as follows:

1. typedef unsigned char BYTE, \*PBYTE, \*LPBYTE;

### CHAR

A CHAR is an 8-bit block of data that typically contains an [**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583) character, as specified in [[ISO/IEC-8859-1]](https://go.microsoft.com/fwlink/?LinkId=90689). For information on the char keyword, see [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 4.2.9.3.

This type is declared as follows:

1. typedef char CHAR, \*PCHAR;

### DOUBLE

A DOUBLE is an 8-byte, double-precision, floating-point number that represents a double-precision, 64-bit [[IEEE754]](https://go.microsoft.com/fwlink/?LinkId=89903) value with the approximate range: +/–5.0 x 10-324 through +/–1.7 x 10308.

The DOUBLE type can also represent not a number (NAN); positive and negative infinity; or positive and negative 0.

This type is declared as follows:

1. typedef double DOUBLE;

### DWORD

A DWORD is a 32-bit unsigned integer (range: 0 through 4294967295 decimal). Because a DWORD is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned long DWORD, \*PDWORD, \*LPDWORD;

### DWORD\_PTR

A DWORD\_PTR is an unsigned long type used for pointer precision. It is used when casting a pointer to an unsigned long type to perform pointer arithmetic. DWORD\_PTR is also commonly used for general 32-bit parameters that have been extended to 64 bits in 64-bit Windows. For more information, see [ULONG\_PTR](#Section_21eec394630d49ed8b4aab74a1614611).

This type is declared as follows:

1. typedef ULONG\_PTR DWORD\_PTR;

### DWORD32

A DWORD32 is a 32-bit unsigned integer.

This type is declared as follows:

1. typedef unsigned int DWORD32;

### DWORD64

A DWORD64 is a 64-bit unsigned integer.

This type is declared as follows:

1. typedef unsigned \_\_int64 DWORD64, \*PDWORD64;

### DWORDLONG

A DWORDLONG is a 64-bit unsigned integer (range: 0 through 18446744073709551615 decimal).

This type is declared as follows:

1. typedef ULONGLONG DWORDLONG, \*PDWORDLONG;

### error\_status\_t

The error\_status\_t return type is used for all methods. This is a Win32 error code.

This type is declared as follows:

1. typedef unsigned long error\_status\_t;

### FLOAT

A **float** is a base type that is specified the IEEE Format section of [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824).section 14.2.

This type is declared as follows:

1. typedef float FLOAT;

### HANDLE

A Handle to an object

This type is declared as follows:

1. typedef void\* HANDLE;

### HCALL

An HCALL is an alias for a [DWORD](#Section_262627d83418462792184ffe110850b2) used to specify a [**handle**](#gt_5044babb-08e3-4bb9-bc12-fe8f542b05ee) to a call, typically used in telephony-related applications.

An HCALL is a 32-bit unsigned integer used to store a handle to a call.

This type is declared as follows:

1. typedef DWORD HCALL;

### HRESULT

An HRESULT is a 32-bit value that is used to describe an error or warning and contains the following fields:

* A 1-bit code that indicates severity, where 0 represents success and 1 represents failure.
* A 4-bit reserved value.
* An 11-bit code, also known as a facility code, that indicates responsibility for the error or warning.
* A 16-bit code that describes the error or warning.

For details on HRESULT values, see [[MS-ERREF]](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90).

This type is declared as follows:

1. typedef LONG HRESULT;

### INT

An INT is a 32-bit signed integer (range: –2147483648 through 2147483647 decimal).

This type is declared as follows:

1. typedef int INT, \*LPINT;

### INT8

An INT8 is an 8-bit signed integer (range: –128 through 127 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef signed char INT8;

### INT16

An INT16 is a 16-bit signed integer (range: –32768 through 32767 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef signed short INT16;

### INT32

An INT32 is a 32-bit signed integer (range: –2147483648 through 2147483647 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef signed int INT32;

### INT64

An INT64 is a 64-bit signed integer (range: –9223372036854775808 through 9223372036854775807 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef signed \_\_int64 INT64;

### LDAP\_UDP\_HANDLE

A handle to an **ADUDPHandle** object that is used to represent the parameters used for communication between a client and [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) servers.

This type is declared as follows:

1. typedef void\* LDAP\_UDP\_HANDLE;

### LMCSTR

A LMCSTR is a 32-bit pointer to a constant null-terminated string of 16-bit [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0).

This type is declared as follows:

1. typedef const wchar\_t\* LMCSTR;

### LMSTR

A LMSTR is a 32-bit pointer to a null-terminated string of 16-bit [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0).

This type is declared as follows:

1. typedef WCHAR\* LMSTR;

### LONG

A LONG is a 32-bit signed integer, in twos-complement format (range: –2147483648 through 2147483647 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef long LONG, \*PLONG, \*LPLONG;

### LONGLONG

A LONGLONG is a 64-bit signed integer (range: –9223372036854775808 through 9223372036854775807 decimal).

This type is declared as follows:

1. typedef signed \_\_int64 LONGLONG;

### LONG\_PTR

A LONG\_PTR is a long type used for pointer precision. It is used when casting a pointer to a long type to perform pointer arithmetic.

This type is declared as follows:

1. typedef \_\_int3264 LONG\_PTR;

### LONG32

A LONG32 is a 32-bit signed integer.

This type is declared as follows:

1. typedef signed int LONG32;

### LONG64

A LONG64 is a 64-bit signed integer.

This type is declared as follows:

1. typedef signed \_\_int64 LONG64, \*PLONG64;

### LPCSTR

An LPCSTR is a 32-bit pointer to a constant null-terminated string of 8-bit Windows ([**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583)) characters.

This type is declared as follows:

1. typedef const char\* LPCSTR;

### LPCVOID

An LPCVOID is a 32-bit pointer to a constant of any type.

This type is declared as follows:

1. typedef const void\* LPCVOID;

### LPCWSTR

An LPCWSTR is a 32-bit pointer to a constant string of 16-bit [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0), which MAY be null-terminated.

This type is declared as follows:

1. typedef const wchar\_t\* LPCWSTR;

### LPSTR

The LPSTR type and its alias PSTR specify a pointer to an array of 8-bit characters, which MAY be terminated by a null character.

In some protocols, it is acceptable to not terminate with a null character, and this option will be indicated in the specification. In this case, the LPSTR or PSTR type MUST either be tagged with the [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) modifier [string], that indicates string semantics, or be accompanied by an explicit length specifier, for example [size\_is()].

The format of the characters MUST be specified by the protocol that uses them. Two common 8-bit formats are [**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583) and [**UTF-8**](#gt_409411c4-b4ed-4ab6-b0ee-6d7815f85a35).

A 32-bit pointer to a string of 8-bit characters, which MAY be null-terminated.

This type is declared as follows:

1. typedef char\* PSTR, \*LPSTR;

### LPWSTR

The LPWSTR type is a 32-bit pointer to a string of 16-bit [**Unicode characters**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0), which MAY be null-terminated. The LPWSTR type specifies a pointer to a sequence of Unicode characters, which MAY be terminated by a null character (usually referred to as "null-terminated Unicode").

In some protocols, an acceptable option is to not terminate a sequence of Unicode characters with a null character. Where this option applies, it is indicated in the protocol specification. In this situation, the LPWSTR or PWSTR type MUST either be tagged with the [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) modifier [string], which indicates string semantics, or MUST be accompanied by an explicit length specifier, as specified in the [RPC\_UNICODE\_STRING (section 2.3.10)](#Section_94a16bb6c6104cb98db626f15f560061) structure.

This type is declared as follows:

1. typedef wchar\_t\* LPWSTR, \*PWSTR;

### NET\_API\_STATUS

The NET\_API\_STATUS type is commonly used as the return value of [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) methods in Microsoft network protocols. See the Win32 error codes as specified in [[MS-ERREF]](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90) for details.

This type is declared as follows:

1. typedef DWORD NET\_API\_STATUS;

### NTSTATUS

NTSTATUS is a standard 32-bit datatype for system-supplied status code values.

NTSTATUS values are used to communicate system information. They are of four types: success values, information values, warnings, and error values, as specified in [[MS-ERREF]](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90).

This type is declared as follows:

1. typedef long NTSTATUS;

### PCONTEXT\_HANDLE

The PCONTEXT\_HANDLE type keeps state information associated with a given client on a server. The state information is called the server's context. Clients can obtain a context handle to identify the server's context for their individual [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) sessions.

A context handle must be of the void \* type, or a type that resolves to void \*. The server program casts it to the required type.

The [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) attribute **[context\_handle]**, as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824), is used to declare PCONTEXT\_HANDLE.

An interface that uses a context handle must have a binding handle for the initial binding, which has to take place before the server can return a context handle. The [handle\_t](#Section_03c032cdc1d14bbeb00cbb1f8da5155b) type is one of the predefined types of the interface definition language (IDL), which is used to create a binding handle.

1. typedef [context\_handle] void\* PCONTEXT\_HANDLE;
2. typedef [ref] PCONTEXT\_HANDLE\* PPCONTEXT\_HANDLE;

### QWORD

A QWORD is a 64-bit unsigned integer.

This type is declared as follows:

1. typedef unsigned \_\_int64 QWORD;

### RPC\_BINDING\_HANDLE

An RPC\_BINDING\_HANDLE is an untyped 32-bit pointer containing information that the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) run-time library uses to access binding information. It is directly equivalent to the type **rpc\_binding\_handle\_t** described in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 3.1.4.

The RPC\_BINDING\_HANDLE data type declares a binding handle containing information that the RPC run-time library uses to access binding information.

The run-time library uses binding information to establish a client/server relationship that allows the execution of remote procedure calls. Based on the context in which a binding handle is created, it is considered a server-binding handle or a client-binding handle.

A server-binding handle contains the information necessary for a client to establish a relationship with a specific server. Any number of RPC API run-time routines return a server-binding handle that can be used for making a remote procedure call.

A client-binding handle cannot be used to make a remote procedure call. The RPC run-time library creates and provides a client-binding handle to a called-server procedure (also called a server-manager routine) as the RPC\_BINDING\_HANDLE parameter. The client-binding handle contains information about the calling client.

This type is declared as follows:

1. typedef void\* RPC\_BINDING\_HANDLE;

### SHORT

A SHORT is a 16-bit signed integer(range: –32768 through 32767 decimal). The first bit (Most Significant Bit (MSB)) is the signing bit.

This type is declared as follows:

1. typedef short SHORT;

### SIZE\_T

**SIZE\_T** is a [ULONG\_PTR](#Section_21eec394630d49ed8b4aab74a1614611) representing the maximum number of bytes to which a pointer can point.

This type is declared as follows:

1. typedef ULONG\_PTR SIZE\_T;

### STRING

Unless otherwise noted, a STRING is a [UCHAR](#Section_050baef1f9784851a3c7ad701a90e54a) buffer that represents a null-terminated string of 8-bit characters.

This type is declared as follows:

1. typedef UCHAR\* STRING;

### UCHAR

A UCHAR is an 8-bit integer with the range: 0 through 255 decimal. Because a UCHAR is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned char UCHAR, \*PUCHAR;

### UINT

A UINT is a 32-bit unsigned integer (range: 0 through 4294967295 decimal). Because a UINT is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned int UINT;

### UINT8

A UINT8 is an 8-bit unsigned integer (range: 0 through 255 decimal). Because a UINT8 is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned char UINT8;

### UINT16

A UINT16 is a 16-bit unsigned integer (range: 0 through 65535 decimal). Because a UINT16 is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned short UINT16;

### UINT32

A UINT32 is a 32-bit unsigned integer (range: 0 through 4294967295 decimal). Because a UINT32 is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned int UINT32;

### UINT64

A UINT64 is a 64-bit unsigned integer (range: 0 through 18446744073709551615 decimal). Because a UINT64 is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned \_\_int64 UINT64;

### ULONG

A ULONG is a 32-bit unsigned integer (range: 0 through 4294967295 decimal). Because a ULONG is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned long ULONG, \*PULONG;

### ULONG\_PTR

A ULONG\_PTR is an unsigned long type used for pointer precision. It is used when casting a pointer to a long type to perform pointer arithmetic.

This type is declared as follows:

1. typedef unsigned \_\_int3264 ULONG\_PTR;

### ULONG32

A ULONG32 is an unsigned **LONG32**.

This type is declared as follows:

1. typedef unsigned int ULONG32;

### ULONG64

A ULONG64 is a 64-bit unsigned integer (range: 0 through 18446744073709551615 decimal). Because a ULONG64 is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned \_\_int64 ULONG64;

### ULONGLONG

A ULONGLONG is a 64-bit unsigned integer (range: 0 through 18446744073709551615 decimal). Because a ULONGLONG is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned \_\_int64 ULONGLONG;

### UNICODE

A single [**Unicode character**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0).

This type is declared as follows:

1. typedef wchar\_t UNICODE;

### UNC

A Universal Naming Convention (UNC) string is used to specify the location of resources such as shared files or devices.

For [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) implementations, this type is declared as follows:

1. typedef STRING UNC;

There are three UNC schemes based on namespace selectors: filespace selector, Win32API selector, and device selector. Only the filespace selector is parsed for on-wire traffic, the other two pass opaque [**BLOBs**](#gt_ad861812-8cb0-497a-80bb-13c95aa4e425) to the consuming entity. The filespace selector is a null-terminated [**Unicode character**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0) string in the following ABNF syntax:

1. UNC = "\\" host-name "\" share-name [ "\" object-name ]
2. host-name = "[" IPv6address ']" / IPv4address / reg-name
3. ; IPv6address, IPv4address, and reg-name as specified in [RFC3986]
4. share-name = 1\*80pchar
5. pchar = %x20-21 / %x23-29 / %x2D-2E / %x30-39 / %x40-5A / %x5E-7B / %x7D-FF
6. object-name = \*path-name [ "\" file-name ]
7. path-name = 1\*255pchar
8. file-name = 1\*255fchar [ ":" stream-name [ ":" stream-type ] ]
9. fchar = %x20-21 / %x23-29 / %x2B-2E / %x30-39 / %x3B / %x3D / %x40-5B / %x5D-7B / %x7D-FF
10. stream-name = \*schar
11. schar = %x01-2E / %x30-39 / %x3B-5B /%x5D-FF
12. stream-type = 1\*schar

**host-name:**   The host name of a server or the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) name of a domain hosting resource, using the syntax of IPv6address, IPv4address, and reg-name as specified in[[RFC3986]](https://go.microsoft.com/fwlink/?LinkId=90453),. The host-name string MUST be a NetBIOS name as specified in [[MS-NBTE]](%5bMS-NBTE%5d.pdf#Section_3461cfa83d284fa38163131bf1046fa3) section 2.2.1, a [**fully qualified domain name (FQDN)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) as specified in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) and [[RFC1123]](https://go.microsoft.com/fwlink/?LinkId=90268), or an IPv4 address as specified in [RFC1123] section 2.1 or an IPv6 address as specified in [[RFC4291]](https://go.microsoft.com/fwlink/?LinkId=90464) section 2.2.

**share-name:**   The name of a [**share**](#gt_a49a79ea-dac7-4016-9a84-cf87161db7e3) or a resource to be accessed. The format of this name depends on the actual file server protocol that is used to access the share. Examples of file server protocols include SMB (as specified in [[MS-SMB]](%5bMS-SMB%5d.pdf#Section_f210069c70864dc2885e861d837df688)), NFS (as specified in [[RFC3530]](https://go.microsoft.com/fwlink/?LinkId=90430)), and NCP (as specified in [NOVELL]).

**object-name:**   The name of an object; this name depends on the actual resource accessed.

The notation "[\**object-name**]\*" indicates that zero or more object names exist in the path, and each object-name is separated from the immediately preceding **object-name** with a backslash path separator. In a UNC path used to access files and directories in an SMB share, for example, **object-name** can be the name of a file or a directory. The **host-name**, **share-name**, and **object-name** are referred to as "pathname components" or "path components". A valid UNC path consists of two or more path components. The **host-name** is referred to as the "first pathname component", the **share-name** as the "second pathname component", and so on. The last component of the path is also referred to as the "leaf component". The protocol that is used to access the resource, and the type of resource that is being accessed, define the size and valid characters for a path component. The only limitations that a [**Distributed File System (DFS)**](#gt_0b8086c9-d025-45b8-bf09-6b5eca72713e) places on path components are that they MUST be at least one character in length and MUST NOT contain a backslash or null.

**path-name**:   One or more pathname components separated by the "\" backslash character. All pathname components other than the last pathname component denote directories or reparse points.

**file-name**:   The "leaf component" of the path, optionally followed by a ":" colon character and a **stream-name** , optionally followed by a ":" colon character and a **stream type**. The **stream-name**, if specified, MAY be zero-length only if **stream-type** is also specified; otherwise, it MUST be at least one character. The **stream-type**, if specified, MUST be at least one character.

### USHORT

A USHORT is a 16-bit unsigned integer (range: 0 through 65535 decimal). Because a USHORT is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned short USHORT;

### VOID

VOID is an alias for **void**.

This type is declared as follows:

1. typedef void VOID, \*PVOID, \*LPVOID;

### WCHAR

A WCHAR is a 16-bit [**Unicode character**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0).

This type is declared as follows:

1. typedef wchar\_t WCHAR, \*PWCHAR;

### WORD

A WORD is a 16-bit unsigned integer (range: 0 through 65535 decimal). Because a WORD is unsigned, its first bit (Most Significant Bit (MSB)) is not reserved for signing.

This type is declared as follows:

1. typedef unsigned short WORD, \*PWORD, \*LPWORD;

## Common Data Structures

This section contains common data structures that are defined in either C, C++, or ABNF.

### EVENT\_DESCRIPTOR

The EVENT\_DESCRIPTOR structure specifies the metadata that defines an event.

1. typedef struct \_EVENT\_DESCRIPTOR {
2. USHORT Id;
3. UCHAR Version;
4. UCHAR Channel;
5. UCHAR Level;
6. UCHAR Opcode;
7. USHORT Task;
8. ULONGLONG Keyword;
9. } EVENT\_DESCRIPTOR,
10. \*PEVENT\_DESCRIPTOR,
11. \*PCEVENT\_DESCRIPTOR;

**Id:**  The event identifier.

**Version:**  The version of the event, which indicates a revision to the event definition. The Version and Id members uniquely identify the event within the scope of a provider.

**Channel:**  Defines the audience for the event (for example, administrator or developer).

**Level:**  Specifies the severity or level of detail included in the event (for example, informational or fatal).

**Opcode:**  Identifies a step in a sequence of operations being performed within a Task.

**Task:**  Identifies a larger unit of work within an application or component (broader in scope than the Opcode).

**Keyword:**  A bitmask that specifies a logical group of related events. Each bit corresponds to one group. An event can belong to one or more groups. The keyword can contain one or more provider-defined keywords, standard keywords, or both.

This structure represents an event defined in a manifest and is included in the [EVENT\_HEADER](#Section_fa4f783606ee4ab68688386a5a85f8c5) structure.

### EVENT\_HEADER

The EVENT\_HEADER structure defines the main parameters of an event.

1. typedef struct \_EVENT\_HEADER {
2. USHORT Size;
3. USHORT HeaderType;
4. USHORT Flags;
5. USHORT EventProperty;
6. ULONG ThreadId;
7. ULONG ProcessId;
8. LARGE\_INTEGER TimeStamp;
9. GUID ProviderId;
10. EVENT\_DESCRIPTOR EventDescriptor;
11. union {
12. struct {
13. ULONG KernelTime;
14. ULONG UserTime;
15. };
16. ULONG64 ProcessorTime;
17. };
18. GUID ActivityId;
19. } EVENT\_HEADER,
20. \*PEVENT\_HEADER;

**Size:**  Size of the event record, in bytes.

**HeaderType:**  Reserved.

**Flags:**  Flags that provide information about the event such as the type of session it was logged to and whether the event contains extended data. This member can contain one or more of the following flags.

| Value | Meaning |
| --- | --- |
| EVENT\_HEADER\_FLAG\_EXTENDED\_INFO | The ExtendedData member of the event record contains data. |
| EVENT\_HEADER\_FLAG\_PRIVATE\_SESSION | The event was logged to a private session. |
| EVENT\_HEADER\_FLAG\_STRING\_ONLY | The event data is a null-terminated Unicode string. |
| EVENT\_HEADER\_FLAG\_TRACE\_MESSAGE | The provider used an implementation-specific trace message function to log the event.Typically indicates that the event was written by the Windows software trace preprocessor. |
| EVENT\_HEADER\_FLAG\_NO\_CPUTIME | Indicates that elapsed execution time was not recorded; the **ProcessorTime** member can be used to determine the elapsed execution time. |
| EVENT\_HEADER\_FLAG\_32\_BIT\_HEADER | Indicates that the provider was running on a 32-bit computer or in a WOW64 session. |
| EVENT\_HEADER\_FLAG\_64\_BIT\_HEADER | Indicates that the provider was running on a 64-bit computer. |
| EVENT\_HEADER\_FLAG\_CLASSIC\_HEADER | Indicates that provider used a trace event function to log the event. |

**EventProperty:**  Indicates the source to use for parsing the event data.

| Value | Meaning |
| --- | --- |
| EVENT\_HEADER\_PROPERTY\_XML | Indicates that you need a manifest to parse the event data. |
| EVENT\_HEADER\_PROPERTY\_FORWARDED\_XML | Indicates that the event data contains within itself a fully rendered XML description of the data, so you do not need a manifest to parse the event data. |
| EVENT\_HEADER\_PROPERTY\_LEGACY\_EVENTLOG | Indicates that you need a WMI MOF class to parse the event data. |

**ThreadId:**  Identifies the thread that generated the event.

**ProcessId:**  Identifies the process that generated the event.

**TimeStamp:**  Contains the time that the event occurred. The resolution is system time unless the **ProcessTraceMode** member of EVENT\_TRACE\_LOGFILE contains the PROCESS\_TRACE\_MODE\_RAW\_TIMESTAMP flag, in which case the resolution depends on the value of the **Wnode.ClientContext** member of EVENT\_TRACE\_PROPERTIES at the time the controller created the session.

**ProviderId:**  GUID that uniquely identifies the provider that logged the event.

**EventDescriptor:**  Defines information about the event such as the event identifier and severity level.

**KernelTime:**  Elapsed execution time for kernel-mode instructions, in CPU time units. For private sessions, the value in the **ProcessorTime** member can be used instead.

**UserTime:**  Elapsed execution time for user-mode instructions, in CPU time units. For private sessions, the value in the **ProcessorTime** member can be used instead.

**ProcessorTime:**  For private sessions, the elapsed execution time for user-mode instructions, in CPU ticks.

**ActivityId:**  Identifier that relates two events.

The **KernelTime** and **UserTime** members can be used to determine the CPU cost in units for a set of instructions (the values indicate the CPU usage charged to that thread at the time of logging). For example, if Event A and Event B are consecutively logged by the same thread and they have CPU usage numbers 150 and 175, then the activity that was performed by that thread between events A and B cost 25 CPU time units (175 – 150).

### FILETIME

The FILETIME structure is a 64-bit value that represents the number of 100-nanosecond intervals that have elapsed since January 1, 1601, Coordinated Universal Time (UTC).

1. typedef struct \_FILETIME {
2. DWORD dwLowDateTime;
3. DWORD dwHighDateTime;
4. } FILETIME,
5. \*PFILETIME,
6. \*LPFILETIME;

**dwLowDateTime:**  A 32-bit unsigned integer that contains the low-order bits of the file time.

**dwHighDateTime:**  A 32-bit unsigned integer that contains the high-order bits of the file time.

### GUID and UUID

A [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1), also known as a [**UUID**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3), is a 16-byte structure, intended to serve as a unique identifier for an object. There are three representations of a GUID, as described in the following sections.

#### GUID--RPC IDL representation

The following structure is an [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) representation of [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) equivalent to and compatible with a DCE UUID ([[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section A.1) according to the following mappings.

1. typedef struct \_GUID {
2. unsigned long Data1;
3. unsigned short Data2;
4. unsigned short Data3;
5. byte Data4[8];
6. } GUID,
7. UUID,
8. \*PGUID;

**Data1:**  This member is generally treated as an opaque value. This member is equivalent to the time\_low field of a DCE UUID ([C706] section A.1).

**Data2:**  This member is generally treated as an opaque value. This member is equivalent to the time\_mid field of a DCE UUID ([C706] section A.1).

**Data3:**  This member is generally treated as an opaque value. This member is equivalent to the time\_hi\_and\_version field of a DCE UUID ([C706] section A.1).

**Data4:**  This array is generally treated as a sequence of opaque values. This member is equivalent to the following sequence of fields of a DCE UUID ([C706] section A.1) in this order: clock\_seq\_hi\_and\_reserved, clock\_seq\_low, and the sequence of bytes in the node field.

#### GUID--Packet Representation

The packet version is used within block protocols. The following diagram represents a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) as an opaque sequence of bytes.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Data1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Data2 | | | | | | | | | | | | | | | | Data3 | | | | | | | | | | | | | | | |
| Data4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Data1 (4 bytes):** The value of the **Data1** member (section [2.3.4](#Section_4926e530816e41c2b251ec5c7aca018a)), in little-endian byte order.

**Data2 (2 bytes):** The value of the **Data2** member (section 2.3.4), in little-endian byte order.

**Data3 (2 bytes):** The value of the **Data3** member (section 2.3.4), in little-endian byte order.

**Data4 (8 bytes):** The value of the **Data4** member (section 2.3.4), in little-endian byte order.

#### GUID--Curly Braced String Representation

The curly braced GUID string representation is a format commonly used for a string representation of the [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) type (as specified in section [2.3.4.1](#Section_49e490b8f97245d6a3a499f924998d97)) is described by the following ABNF syntax, as specified in [[RFC5234]](https://go.microsoft.com/fwlink/?LinkId=123096).

1. CurlyBraceGuidString = "{" UUID "}"

Where [**UUID**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) represents the string form of a UUID, as specified in [[RFC4122]](https://go.microsoft.com/fwlink/?LinkId=90460) section 3. The non-terminal symbol CurlyBraceGuidString represents (that is, generates) strings that satisfy the definition of [**curly braced GUID string**](#gt_b753d3f3-f3b7-4fee-bf4d-63085e108ec9).

By way of illustration, the UUID string specified in [RFC4122] section 3 as an example would have the following representation as a curly braced GUID string.

1. {f81d4fae-7dec-11d0-a765-00a0c91e6bf6}

### LARGE\_INTEGER

The LARGE\_INTEGER structure is used to represent a 64-bit signed integer value.

1. typedef struct \_LARGE\_INTEGER {
2. signed \_\_int64 QuadPart;
3. } LARGE\_INTEGER,
4. \*PLARGE\_INTEGER;

### LCID

A language code identifier structure is stored as a [DWORD](#Section_262627d83418462792184ffe110850b2). The lower word contains the language identifier, and the upper word contains both the sorting identifier (ID) and a reserved value. For additional details about the structure and possible values, see [[MS-LCID]](%5bMS-LCID%5d.pdf#Section_70feba9f294e491eb6eb56532684c37f).

This type is declared as follows:

1. typedef DWORD LCID;

### LUID

The LUID structure is 64-bit value guaranteed to be unique only on the system on which it was generated. The uniqueness of a locally unique identifier (LUID) is guaranteed only until the system is restarted.

1. typedef struct \_LUID {
2. DWORD LowPart;
3. LONG HighPart;
4. } LUID,
5. \*PLUID;

**LowPart:**  The low-order bits of the structure.

**HighPart:**  The high-order bits of the structure.

### MULTI\_SZ

The MULTI\_SZ structure defines an implementation-specific[<2>](#Appendix_A_2" \o "Product behavior note 2) type that contains a sequence of null-terminated strings, terminated by an empty string (\0) so that the last two characters are both null terminators.

1. typedef struct \_MULTI\_SZ {
2. wchar\_t\* Value;
3. DWORD nChar;
4. } MULTI\_SZ;

**Value:**  A data buffer, which is a string literal containing multiple null-terminated strings serially.

**nChar:**  The length, in characters, including the two terminating nulls.

### OBJECT\_TYPE\_LIST

The OBJECT\_TYPE\_LIST structure identifies an object type element in a hierarchy of object types. The [Access Check Algorithm Pseudocode](#Section_4f1bbcbb814a4c70a11e2a5b8779a6f9) functions (section 2.5.3.2) use an array of OBJECT\_TYPE\_LIST structures to define a hierarchy of an object and its sub-objects, such as property sets and properties.

1. typedef struct \_OBJECT\_TYPE\_LIST {
2. WORD Level;
3. ACCESS\_MASK Remaining;
4. GUID\* ObjectType;
5. } OBJECT\_TYPE\_LIST,
6. \*POBJECT\_TYPE\_LIST;

**Level:**  Specifies the level of the object type in the hierarchy of an object and its sub-objects. Level zero indicates the object itself. Level one indicates a sub-object of the object, such as a property set. Level two indicates a sub-object of the level one sub-object, such as a property. There can be a maximum of five levels numbered zero through four.

| Value | Meaning |
| --- | --- |
| ACCESS\_OBJECT\_GUID  0x0 | Indicates the object itself at level zero. |
| ACCESS\_PROPERTY\_SET\_GUID  0x1 | Indicates a property set at level one. |
| ACCESS\_PROPERTY\_GUID  0x2 | Indicates a property at level two. |
| ACCESS\_MAX\_LEVEL  0x4 | Maximum level. |

**Remaining:**  Remaining access bits for this element, used by the access check algorithm, as specified in section 2.5.3.2.

**ObjectType:**  A pointer to the [GUID](#Section_49e490b8f97245d6a3a499f924998d97) for the object or sub-object.

### RPC\_UNICODE\_STRING

The RPC\_UNICODE\_STRING structure specifies a [**Unicode string**](#gt_b069acb4-e364-453e-ac83-42d469bb339e). This structure is defined in [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) as follows:

1. typedef struct \_RPC\_UNICODE\_STRING {
2. unsigned short Length;
3. unsigned short MaximumLength;
4. [size\_is(MaximumLength/2), length\_is(Length/2)]
5. WCHAR\* Buffer;
6. } RPC\_UNICODE\_STRING,
7. \*PRPC\_UNICODE\_STRING;

**Length:**  The length, in bytes, of the string pointed to by the **Buffer** member, not including the terminating null character if any. The length MUST be a multiple of 2. The length SHOULD equal the entire size of the **Buffer**, in which case there is no terminating null character. Any method that accesses this structure MUST use the **Length** specified instead of relying on the presence or absence of a null character.

**MaximumLength:**  The maximum size, in bytes, of the string pointed to by **Buffer**. The size MUST be a multiple of 2. If not, the size MUST be decremented by 1 prior to use. This value MUST not be less than **Length**.

**Buffer:**  A pointer to a string buffer. If **MaximumLength** is greater than zero, the buffer MUST contain a non-null value.

### SERVER\_INFO\_100

The SERVER\_INFO\_100 structure contains information about the specified server, including the name and platform.

1. typedef struct \_SERVER\_INFO\_100 {
2. DWORD sv100\_platform\_id;
3. [string] wchar\_t\* sv100\_name;
4. } SERVER\_INFO\_100,
5. \*PSERVER\_INFO\_100,
6. \*LPSERVER\_INFO\_100;

**sv100\_platform\_id:**  Specifies the information level to use for platform-specific information.

| Name | Value |
| --- | --- |
| PLATFORM\_ID\_DOS | 300 |
| PLATFORM\_ID\_OS2 | 400 |
| PLATFORM\_ID\_NT | 500 |
| PLATFORM\_ID\_OSF | 600 |
| PLATFORM\_ID\_VMS | 700 |

**sv100\_name:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) [**UTF-16**](#gt_4c9eef52-69d4-43e7-ac04-ff1fe43a94fb) [**Internet host name**](#gt_4d5d5403-372f-4f9f-8d7a-65c310c807d9) or [**NetBIOS host name**](#gt_150cc108-7e58-4fdb-957d-2a3734ba15f5) of a server.

### SERVER\_INFO\_101

The SERVER\_INFO\_101 structure contains information about the specified server, including the name, platform, type of server, and associated software.

1. typedef struct \_SERVER\_INFO\_101 {
2. DWORD sv101\_platform\_id;
3. [string] wchar\_t\* sv101\_name;
4. DWORD sv101\_version\_major;
5. DWORD sv101\_version\_minor;
6. DWORD sv101\_version\_type;
7. [string] wchar\_t\* sv101\_comment;
8. } SERVER\_INFO\_101,
9. \*PSERVER\_INFO\_101,
10. \*LPSERVER\_INFO\_101;

**sv101\_platform\_id:**  Specifies the information level to use for platform-specific information.

| Name | Value |
| --- | --- |
| PLATFORM\_ID\_DOS | 300 |
| PLATFORM\_ID\_OS2 | 400 |
| PLATFORM\_ID\_NT | 500 |
| PLATFORM\_ID\_OSF | 600 |
| PLATFORM\_ID\_VMS | 700 |

**sv101\_name:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) [**UTF-16**](#gt_4c9eef52-69d4-43e7-ac04-ff1fe43a94fb) [**Internet host name**](#gt_4d5d5403-372f-4f9f-8d7a-65c310c807d9) or [**NetBIOS host name**](#gt_150cc108-7e58-4fdb-957d-2a3734ba15f5) of a server.

**sv101\_version\_major:**  Specifies the major release version number of the operating system. The server MUST set this field to an implementation-specific major release version number that corresponds to the host operating system as specified in the following table.

| Operating System | Major version |
| --- | --- |
| Windows NT 4.0 operating system | 4 |
| Windows 2000 operating system | 5 |
| Windows XP operating system | 5 |
| Windows Server 2003 operating system | 5 |
| Windows Vista operating system | 6 |
| Windows Server 2008 operating system | 6 |
| Windows Server 2008 R2 operating system | 6 |

**sv101\_version\_minor:**  Specifies the minor release version number of the operating system. The server MUST set this field to an implementation-specific minor release version number that corresponds to the host operating system as specified in the following table.

| Operating System | Minor version |
| --- | --- |
| Windows NT 4.0 | 0 |
| Windows 2000 | 0 |
| Windows XP | 1 |
| Windows Server 2003 | 2 |
| Windows Vista | 0 |
| Windows Server 2008 | 0 |
| Windows Server 2008 R2 | 1 |

**sv101\_version\_type:**  The sv101\_version\_type field specifies the SV\_TYPE flags, which indicate the software services that are available (but not necessarily running) on the server. This member MUST be a combination of one or more of the following values.

| Constant/Value | Description |
| --- | --- |
| SV\_TYPE\_WORKSTATION  0x00000001 | A server running the WorkStation Service. |
| SV\_TYPE\_SERVER  0x00000002 | A server running the Server Service. |
| SV\_TYPE\_SQLSERVER  0x00000004 | A server running SQL Server. |
| SV\_TYPE\_DOMAIN\_CTRL  0x00000008 | A primary domain controller. |
| SV\_TYPE\_DOMAIN\_BAKCTRL  0x00000010 | A backup domain controller. |
| SV\_TYPE\_TIME\_SOURCE  0x00000020 | A server is available as a time source for network time synchronization. |
| SV\_TYPE\_AFP  0x00000040 | An Apple File Protocol server. |
| SV\_TYPE\_NOVELL  0x00000080 | A Novell server. |
| SV\_TYPE\_DOMAIN\_MEMBER  0x00000100 | A LAN Manager 2.x domain member. |
| SV\_TYPE\_PRINTQ\_SERVER  0x00000200 | A server sharing print queue. |
| SV\_TYPE\_DIALIN\_SERVER  0x00000400 | A server running a dial-in service. |
| SV\_TYPE\_XENIX\_SERVER  0x00000800 | A Xenix server. |
| SV\_TYPE\_NT  0x00001000 | Windows Server 2003, Windows XP, Windows 2000, or Windows NT operating system. |
| SV\_TYPE\_WFW  0x00002000 | A server running Windows for Workgroups. |
| SV\_TYPE\_SERVER\_MFPN  0x00004000 | Microsoft File and Print for NetWare. |
| SV\_TYPE\_SERVER\_NT  0x00008000 | Windows Server 2003, Windows 2000 Server operating system, or a server that is not a domain controller. |
| SV\_TYPE\_POTENTIAL\_BROWSER  0x00010000 | A server that can run the browser service. |
| SV\_TYPE\_BACKUP\_BROWSER  0x00020000 | A server running a browser service as backup. |
| SV\_TYPE\_MASTER\_BROWSER  0x00040000 | A server running the master browser service. |
| SV\_TYPE\_DOMAIN\_MASTER  0x00080000 | A server running the domain master browser. |
| SV\_TYPE\_WINDOWS  0x00400000 | Windows Millennium Edition operating system, Windows 98 operating system, or Windows 95. |
| SV\_TYPE\_TERMINALSERVER  0x02000000 | Terminal Server. |
| SV\_TYPE\_CLUSTER\_VS\_NT  0x04000000 | Cluster virtual servers available in the domain. |
| SV\_TYPE\_LOCAL\_LIST\_ONLY  0x40000000 | Servers maintained by the browser. |
| SV\_TYPE\_DOMAIN\_ENUM  0x80000000 | Primary domain. |
| SV\_TYPE\_ALL  0xFFFFFFFF | All servers. |

**sv101\_comment:**  A pointer to a null-terminated Unicode UTF-16 string that specifies a comment that describes the server.

### SYSTEMTIME

The SYSTEMTIME structure is a date and time, in Coordinated Universal Time (UTC), represented by using individual [WORD](#Section_f8573df3a44a4a50b070ac4c3aa78e3c)-sized structure members for the month, day, year, day of week, hour, minute, second, and millisecond.

1. typedef struct \_SYSTEMTIME {
2. WORD wYear;
3. WORD wMonth;
4. WORD wDayOfWeek;
5. WORD wDay;
6. WORD wHour;
7. WORD wMinute;
8. WORD wSecond;
9. WORD wMilliseconds;
10. } SYSTEMTIME,
11. \*PSYSTEMTIME;

### UINT128

The UINT128 structure is intended to hold 128-bit unsigned integers, such as an IPv6 destination address.

1. typedef struct \_UINT128 {
2. UINT64 lower;
3. UINT64 upper;
4. } UINT128,
5. \*PUINT128;

### ULARGE\_INTEGER

The ULARGE\_INTEGER structure is used to represent a 64-bit unsigned integer value.

1. typedef struct \_ULARGE\_INTEGER {
2. unsigned \_\_int64 QuadPart;
3. } ULARGE\_INTEGER,
4. \*PULARGE\_INTEGER;

## Constructed Security Types

The following types are used to specify structures that are specific to the Windows security model.

### SID\_IDENTIFIER\_AUTHORITY

The SID\_IDENTIFIER\_AUTHORITY structure represents the top-level authority of a security identifier (SID).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Value | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | |

**Value (6 bytes):** An array of six 8-bit unsigned integers that specify the top-level authority of a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25), [RPC\_SID](#Section_5cb97814a1c24215b7dc76d1f4bfad01), and LSAPR\_SID\_INFORMATION.

The identifier authority value identifies the domain security authority that issued the SID. The following identifier authorities are predefined for wire traffic.

| Identifier Authority | Meaning |
| --- | --- |
| NULL\_SID\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x00} | Specifies the **NULL** SID authority. It defines only the **NULL** well-known-SID: S-1-0-0. |
| WORLD\_SID\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x01} | Specifies the World SID authority. It only defines the **Everyone** well-known-SID: S-1-1-0. |
| LOCAL\_SID\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x02} | Specifies the Local SID authority. It defines only the **Local** well-known-SID: S-1-2-0. |
| CREATOR\_SID\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x03} | Specifies the Creator SID authority. It defines the **Creator Owner**, **Creator Group**, and **Creator Owner Server** well-known-SIDs: S-1-3-0, S-1-3-1, and S-1-3-2. These SIDs are used as placeholders in an access control list (ACL) and are replaced by the user, group, and machine SIDs of the security principal. |
| NON\_UNIQUE\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x04} | Not used. |
| SECURITY\_NT\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x05} | Specifies the Windows NT security subsystem SID authority. It defines all other SIDs in the forest. |
| SECURITY\_APP\_PACKAGE\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x0F} | Specifies the application package authority. It defines application capability SIDs. |
| SECURITY\_MANDATORY\_LABEL\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x10} | Specifies the Mandatory label authority. It defines the integrity level SIDs. |
| SECURITY\_SCOPED\_POLICY\_ID\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x11} | Specifies the Scoped Policy Authority. It defines all other scoped policy SIDs in the forest.[<3>](#Appendix_A_3" \o "Product behavior note 3) |
| SECURITY\_AUTHENTICATION\_AUTHORITY  {0x00, 0x00, 0x00, 0x00, 0x00, 0x12} | Specifies the authentication authority asserting the client’s identity. It defines only the following well-known SIDs: S-1-18-1, and S-1-18-2.[<4>](#Appendix_A_4" \o "Product behavior note 4) |

#### RPC\_SID\_IDENTIFIER\_AUTHORITY

The RPC\_SID\_IDENTIFIER\_AUTHORITY structure is a representation of a security identifier (SID) authority, as specified by the [SID\_IDENTIFIER\_AUTHORITY](#Section_c6ce42753d904890ab3a514745e4637e) structure. This structure is defined in [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) as follows.

1. typedef struct \_RPC\_SID\_IDENTIFIER\_AUTHORITY {
2. byte Value[6];
3. } RPC\_SID\_IDENTIFIER\_AUTHORITY;

For individual member semantics of the SID\_IDENTIFIER\_AUTHORITY structure, see section 2.4.1.

### SID

A security identifier (SID) uniquely identifies a security principal. Each security principal has a unique SID that is issued by a security agent. The agent can be a Windows local system or domain. The agent generates the SID when the security principal is created. The SID can be represented as a character string or as a structure. When represented as strings, for example in documentation or logs, SIDs are expressed as follows:

1. S-1-IdentifierAuthority-SubAuthority1-SubAuthority2-...-SubAuthorityn

The top-level issuer is the authority. Each issuer specifies, in an implementation-specific manner, how many integers identify the next issuer.

A newly created account store is assigned a 96-bit identifier (a cryptographic strength (pseudo) random number).

A newly created security principal in an account store is assigned a 32-bit identifier that is unique within the store.

The last item in the series of **SubAuthority** values is known as the **relative identifier (RID)**. Differences in the **RID** are what distinguish the different SIDs generated within a domain.

Consumers of SIDs SHOULD NOT rely on anything more than that the SID has the appropriate structure.

The formal string syntax is given in section [2.4.2.1](#Section_c92a27b1c7724fa7a43215df5f1b66a1).

The packet representation of the SID structure used by block protocols is defined in section [2.4.2.2](#Section_f992ad600fe44b879fedbeb478836861).

The RPC marshaled version of the SID structure is defined in section [2.4.2.3](#Section_5cb97814a1c24215b7dc76d1f4bfad01).

#### SID String Format Syntax

The SID string format syntax, a format commonly used for a string representation of the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) type (as specified in section 2.4.2), is described by the following ABNF syntax, as specified in [[RFC5234]](https://go.microsoft.com/fwlink/?LinkId=123096).

1. SID= "S-1-" IdentifierAuthority 1\*SubAuthority
2. IdentifierAuthority= IdentifierAuthorityDec / IdentifierAuthorityHex
3. ; If the identifier authority is < 2^32, the
4. ; identifier authority is represented as a decimal
5. ; number
6. ; If the identifier authority is >= 2^32,
7. ; the identifier authority is represented in
8. ; hexadecimal
9. IdentifierAuthorityDec = 1\*10DIGIT
10. ; IdentifierAuthorityDec, top level authority of a
11. ; security identifier is represented as a decimal number
12. IdentifierAuthorityHex = "0x" 12HEXDIG
13. ; IdentifierAuthorityHex, the top-level authority of a
14. ; security identifier is represented as a hexadecimal number
15. SubAuthority= "-" 1\*10DIGIT
16. ; Sub-Authority is always represented as a decimal number
17. ; No leading "0" characters are allowed when IdentifierAuthority
18. ; or SubAuthority is represented as a decimal number
19. ; All hexadecimal digits must be output in string format,
20. ; pre-pended by "0x"

#### SID--Packet Representation

This is a packet representation of the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) type (as specified in section 2.4.2) for use by block protocols. Multiple-byte fields are transmitted on the wire with an endianness specified by the protocol in question.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Revision | | | | | | | | SubAuthorityCount | | | | | | | | IdentifierAuthority | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SubAuthority (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Revision (1 byte):** An 8-bit unsigned integer that specifies the revision level of the SID. This value MUST be set to 0x01.

**SubAuthorityCount (1 byte):** An 8-bit unsigned integer that specifies the number of elements in the **SubAuthority** array. The maximum number of elements allowed is 15.

**IdentifierAuthority (6 bytes):** A [SID\_IDENTIFIER\_AUTHORITY](#Section_c6ce42753d904890ab3a514745e4637e) structure that indicates the authority under which the SID was created. It describes the entity that created the SID. The Identifier Authority value {0,0,0,0,0,5} denotes SIDs created by the NT SID authority.

**SubAuthority (variable):** A variable length array of unsigned 32-bit integers that uniquely identifies a principal relative to the **IdentifierAuthority**. Its length is determined by **SubAuthorityCount**.

#### RPC\_SID

The RPC\_SID structure is an IDL representation of the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) type (as specified in section 2.4.2) for use by RPC-based protocols.

1. typedef struct \_RPC\_SID {
2. unsigned char Revision;
3. unsigned char SubAuthorityCount;
4. RPC\_SID\_IDENTIFIER\_AUTHORITY IdentifierAuthority;
5. [size\_is(SubAuthorityCount)] unsigned long SubAuthority[];
6. } RPC\_SID,
7. \*PRPC\_SID,
8. \*PSID;

**Revision:**  An 8-bit unsigned integer that specifies the revision level of the SID. This value MUST be set to 0x01.

**SubAuthorityCount:**  An 8-bit unsigned integer that specifies the number of elements in the **SubAuthority** array. The maximum number of elements allowed is 15.

**IdentifierAuthority:**  An [RPC\_SID\_IDENTIFIER\_AUTHORITY](#Section_d7e6e5a5437c41e58ba1bdfd43e96cbc) structure that indicates the authority under which the SID was created. It describes the entity that created the SID. The Identifier Authority value {0,0,0,0,0,5} denotes SIDs created by the NT SID authority.

**SubAuthority:**  A variable length array of unsigned 32-bit integers that uniquely identifies a principal relative to the **IdentifierAuthority**. Its length is determined by **SubAuthorityCount**.

#### Well-Known SID Structures

Well-known SID structures are a group of [SIDs](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identify generic users or generic groups. Their values remain constant across all operating systems.

The *<root-domain>* identifier represents the three sub-authority values associated with the root domain, which is the first domain that is created in an Active Directory forest infrastructure. The *<domain>* identifier represents the three sub-authority values associated with any domain, and the *<machine>* identifier represents the three sub-authority values associated with a specific machine. Root domain–based groups like the Enterprise and Schema administrators have forestwide permissions.

For example, given a SID defined in the table below as S-1-5-21-<domain>-513, and the actual instance of the domain having the three sub authority values of 1, 2, and 3:

**S-1**: Indicates a revision or version 1 SID.

**5**: SECURITY\_NT\_AUTHORITY, indicates it's a Windows specific SID.

**21**: SECURITY\_NT\_NON\_UNIQUE, indicates a domain id will follow.

**1-2-3**: The next three **SubAuthority** arrays contain 32-bit random numbers to uniquely identify the domain.

**RID**: Indicates a unique object ID within the domain.

The actual constructed SID would be S-1-5-21-1-2-3-513.

The following table lists well-known SID structure values and their matching descriptions.

| Constant/value | Description |
| --- | --- |
| NULL  S-1-0-0 | No Security principal. |
| EVERYONE  S-1-1-0 | A group that includes all users. |
| LOCAL  S-1-2-0 | A group that includes all users who have logged on locally. |
| CONSOLE\_LOGON  S-1-2-1 | A group that includes users who are logged on to the physical console. This SID can be used to implement security policies that grant different rights based on whether a user has been granted physical access to the console.[<5>](#Appendix_A_5" \o "Product behavior note 5) |
| CREATOR\_OWNER  S-1-3-0 | A placeholder in an inheritable [access control entry (ACE)](#Section_d06e5a81176e46c69cf79137aad4455e). When the ACE is inherited, the system replaces this SID with the SID for the object's creator. |
| CREATOR\_GROUP  S-1-3-1 | A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's creator. |
| OWNER\_SERVER  S-1-3-2 | A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the object's owner server.[<6>](#Appendix_A_6" \o "Product behavior note 6) |
| GROUP\_SERVER  S-1-3-3 | A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the object's group server.[<7>](#Appendix_A_7" \o "Product behavior note 7) |
| OWNER\_RIGHTS  S-1-3-4 | A group that represents the current owner of the object. When an ACE that carries this SID is applied to an object, the system ignores the implicit READ\_CONTROL and WRITE\_DAC permissions for the object owner. |
| NT\_AUTHORITY  S-1-5 | A SID containing only the SECURITY\_NT\_AUTHORITY identifier authority. |
| DIALUP  S-1-5-1 | A group that includes all users who have logged on through a dial-up connection. |
| NETWORK  S-1-5-2 | A group that includes all users who have logged on through a network connection. |
| BATCH  S-1-5-3 | A group that includes all users who have logged on through a batch queue facility. |
| INTERACTIVE  S-1-5-4 | A group that includes all users who have logged on interactively. |
| LOGON\_ID  S-1-5-5-x-y | A logon session. The X and Y values for these SIDs are different for each logon session and are recycled when the operating system is restarted. |
| SERVICE  S-1-5-6 | A group that includes all security principals that have logged on as a service. |
| ANONYMOUS  S-1-5-7 | A group that represents an anonymous logon. |
| PROXY  S-1-5-8 | Identifies a SECURITY\_NT\_AUTHORITY Proxy.[<8>](#Appendix_A_8" \o "Product behavior note 8) |
| ENTERPRISE\_DOMAIN\_CONTROLLERS  S-1-5-9 | A group that includes all domain controllers in a forest that uses an Active Directory directory service. |
| PRINCIPAL\_SELF  S-1-5-10 | A placeholder in an inheritable ACE on an account object or group object in Active Directory. When the ACE is inherited, the system replaces this SID with the SID for the security principal that holds the account. |
| AUTHENTICATED\_USERS  S-1-5-11 | A group that includes all users whose identities were authenticated when they logged on. |
| RESTRICTED\_CODE  S-1-5-12 | This SID is used to control access by untrusted code. [ACL](#Section_20233ed8a6c64097aafadd545ed24428) validation against tokens with RC consists of two checks, one against the token's normal list of SIDs and one against a second list (typically containing RC - the "RESTRICTED\_CODE" token - and a subset of the original token SIDs). Access is granted only if a token passes both tests. Any ACL that specifies RC must also specify WD - the "EVERYONE" token. When RC is paired with WD in an ACL, a superset of "EVERYONE", including untrusted code, is described. |
| TERMINAL\_SERVER\_USER  S-1-5-13 | A group that includes all users who have logged on to a Terminal Services server. |
| REMOTE\_INTERACTIVE\_LOGON  S-1-5-14 | A group that includes all users who have logged on through a terminal services logon. |
| THIS\_ORGANIZATION  S-1-5-15 | A group that includes all users from the same [**organization**](#gt_6fae7775-5232-4206-b452-f298546ab54f). If this SID is present, the OTHER\_ORGANIZATION SID MUST NOT be present.[<9>](#Appendix_A_9" \o "Product behavior note 9) |
| IUSR  S-1-5-17 | An account that is used by the default Internet Information Services (IIS) user. |
| LOCAL\_SYSTEM  S-1-5-18 | An account that is used by the operating system. |
| LOCAL\_SERVICE  S-1-5-19 | A local service account. |
| NETWORK\_SERVICE  S-1-5-20 | A network service account. |
| ENTERPRISE\_READONLY\_DOMAIN\_CONTROLLERS  S-1-5-21-*<root domain>*-498 | A universal group containing all read-only domain controllers in a forest. |
| COMPOUNDED\_AUTHENTICATION  S-1-5-21-0-0-0-496 | Device identity is included in the Kerberos service ticket. If a forest boundary was crossed, then claims transformation occurred.[<10>](#Appendix_A_10" \o "Product behavior note 10) |
| CLAIMS\_VALID  S-1-5-21-0-0-0-497 | Claims were queried for in the account's domain, and if a forest boundary was crossed, then claims transformation occurred.[<11>](#Appendix_A_11" \o "Product behavior note 11) |
| ADMINISTRATOR  S-1-5-21-*<machine>*-500 | A user account for the system administrator. By default, it is the only user account that is given full control over the system. |
| GUEST  S-1-5-21-*<machine>*-501 | A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled. |
| KRBTGT S-1-5-21-*<domain>*-502 | A service account that is used by the Key Distribution Center (KDC) service. |
| DOMAIN\_ADMINS  S-1-5-21-*<domain>*-512 | A global group whose members are authorized to administer the domain. By default, the DOMAIN\_ADMINS group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. DOMAIN\_ADMINS is the default owner of any object that is created by any member of the group. |
| DOMAIN\_USERS  S-1-5-21-*<domain>*-513 | A global group that includes all user accounts in a domain. |
| DOMAIN\_GUESTS  S-1-5-21-*<domain>*-514 | A global group that has only one member, which is the built-in Guest account of the domain. |
| DOMAIN\_COMPUTERS  S-1-5-21-*<domain>*-515 | A global group that includes all clients and servers that have joined the domain. |
| DOMAIN\_DOMAIN\_CONTROLLERS  S-1-5-21-*<domain>*-516 | A global group that includes all domain controllers in the domain. |
| CERT\_PUBLISHERS  S-1-5-21-*<domain>*-517 | A global group that includes all computers that are running an enterprise certification authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory. |
| SCHEMA\_ADMINISTRATORS  S-1-5-21-*<root-domain>*-518 | A universal group in a native-mode domain, or a global group in a mixed-mode domain. The group is authorized to make schema changes in Active Directory. |
| ENTERPRISE\_ADMINS  S-1-5-21-*<root-domain>*-519 | A universal group in a native-mode domain, or a global group in a mixed-mode domain. The group is authorized to make forestwide changes in Active Directory, such as adding child domains. |
| GROUP\_POLICY\_CREATOR\_OWNERS  S-1-5-21-*<domain>*-520 | A global group that is authorized to create new Group Policy Objects in Active Directory. |
| READONLY\_DOMAIN\_CONTROLLERS  S-1-5-21-*<domain>*-521 | A global group that includes all read-only domain controllers. |
| CLONEABLE\_CONTROLLERS  S-1-5-21-*<domain>*-522 | A global group that includes all domain controllers in the domain that can be cloned. |
| PROTECTED\_USERS  S-1-5-21-*<domain>*-525 | A global group that is afforded additional protections against authentication security threats.[<12>](#Appendix_A_12" \o "Product behavior note 12) For more information, see [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) and [[MS-KILE]](%5bMS-KILE%5d.pdf#Section_2a32282edd484ad9a542609804b02cc9). |
| KEY\_ADMINS  S-1-5-21-*<domain>*-526 | A security group for delegated write access on the msdsKeyCredentialLink attribute only. The group is intended for use in scenarios where trusted external authorities (for example, Active Directory Federated Services) are responsible for modifying this attribute. Only trusted administrators should be made a member of this group.[<13>](#Appendix_A_13" \o "Product behavior note 13) |
| ENTERPRISE\_KEY\_ADMINS  S-1-5-21-*<domain>*-527 | A security group for delegated write access on the msdsKeyCredentialLink attribute only. The group is intended for use in scenarios where trusted external authorities (for example, Active Directory Federated Services) are responsible for modifying this attribute. Only trusted enterprise administrators should be made a member of this group.[<14>](#Appendix_A_14" \o "Product behavior note 14) |
| RAS\_SERVERS  S-1-5-21-*<domain>*-553 | A domain local group for [**Remote Access Services (RAS) servers**](#gt_f8c23490-c220-4d75-a9bd-db04e8fc1c48). By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group. |
| ALLOWED\_RODC\_PASSWORD\_REPLICATION\_GROUP  S-1-5-21-*<domain>*-571 | Members in this group can have their passwords replicated to all read-only domain controllers in the domain.[<15>](#Appendix_A_15" \o "Product behavior note 15) |
| DENIED\_RODC\_PASSWORD\_REPLICATION\_GROUP  S-1-5-21-*<domain>*-572 | Members in this group cannot have their passwords replicated to all read-only domain controllers in the domain.[<16>](#Appendix_A_16" \o "Product behavior note 16) |
| BUILTIN\_ADMINISTRATORS  S-1-5-32-544 | A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Administrators group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Administrators group also is added to the Administrators group. |
| BUILTIN\_USERS  S-1-5-32-545 | A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer. |
| BUILTIN\_GUESTS  S-1-5-32-546 | A built-in group. The Guests group allows users to log on with limited privileges to a computer's built-in Guest account. |
| POWER\_USERS  S-1-5-32-547 | A built-in group. Power users can perform the following actions:   * Create local users and groups. * Modify and delete accounts that they have created. * Remove users from the Power Users, Users, and Guests groups. * Install programs. * Create, manage, and delete local printers. * Create and delete file shares. |
| ACCOUNT\_OPERATORS  S-1-5-32-548 | A built-in group that exists only on domain controllers. Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units of Active Directory except the Built-in container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Administrators groups, nor do they have permission to modify the accounts for members of those groups. |
| SERVER\_OPERATORS  S-1-5-32-549 | A built-in group that exists only on domain controllers. Server Operators can perform the following actions:   * Log on to a server interactively. * Create and delete network shares. * Start and stop services. * Back up and restore files. * Format the hard disk of a computer. * Shut down the computer. |
| PRINTER\_OPERATORS  S-1-5-32-550 | A built-in group that exists only on domain controllers. Print Operators can manage printers and document queues. |
| BACKUP\_OPERATORS  S-1-5-32-551 | A built-in group. Backup Operators can back up and restore all files on a computer, regardless of the permissions that protect those files. |
| REPLICATOR  S-1-5-32-552 | A built-in group that is used by the File Replication Service (FRS) on domain controllers. |
| ALIAS\_PREW2KCOMPACC  S-1-5-32-554 | A backward compatibility group that allows read access on all users and groups in the domain.[<17>](#Appendix_A_17" \o "Product behavior note 17) |
| REMOTE\_DESKTOP  S-1-5-32-555 | An alias. Members of this group are granted the right to log on remotely.[<18>](#Appendix_A_18" \o "Product behavior note 18) |
| NETWORK\_CONFIGURATION\_OPS  S-1-5-32-556 | An alias. Members of this group can have some administrative privileges to manage configuration of networking features.[<19>](#Appendix_A_19" \o "Product behavior note 19) |
| INCOMING\_FOREST\_TRUST\_BUILDERS  S-1-5-32-557 | An alias. Members of this group can create incoming, one-way trusts to this forest.[<20>](#Appendix_A_20" \o "Product behavior note 20) |
| PERFMON\_USERS  S-1-5-32-558 | An alias. Members of this group have remote access to monitor this computer.[<21>](#Appendix_A_21" \o "Product behavior note 21) |
| PERFLOG\_USERS  S-1-5-32-559 | An alias. Members of this group have remote access to schedule the logging of performance counters on this computer.[<22>](#Appendix_A_22" \o "Product behavior note 22) |
| WINDOWS\_AUTHORIZATION\_ACCESS\_GROUP  S-1-5-32-560 | An alias. Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects.[<23>](#Appendix_A_23" \o "Product behavior note 23) |
| TERMINAL\_SERVER\_LICENSE\_SERVERS  S-1-5-32-561 | An alias. A group for Terminal Server License Servers.[<24>](#Appendix_A_24" \o "Product behavior note 24) |
| DISTRIBUTED\_COM\_USERS  S-1-5-32-562 | An alias. A group for [**COM**](#gt_ef2ebebc-1760-407a-9ace-af48f9050e02) to provide computer-wide access controls that govern access to all call, activation, or launch requests on the computer.[<25>](#Appendix_A_25" \o "Product behavior note 25) |
| IIS\_IUSRS  S-1-5-32-568 | A built-in group account for IIS users. |
| CRYPTOGRAPHIC\_OPERATORS  S-1-5-32-569 | A built-in group account for cryptographic operators.[<26>](#Appendix_A_26" \o "Product behavior note 26) |
| EVENT\_LOG\_READERS  S-1-5-32-573 | A built-in local group. Members of this group can read event logs from the local machine.[<27>](#Appendix_A_27" \o "Product behavior note 27) |
| CERTIFICATE\_SERVICE\_DCOM\_ACCESS  S-1-5-32-574 | A built-in local group. Members of this group are allowed to connect to Certification Authorities in the enterprise.[<28>](#Appendix_A_28" \o "Product behavior note 28) |
| RDS\_REMOTE\_ACCESS\_SERVERS  S-1-5-32-575 | Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers and RD Web Access servers used in the deployment need to be in this group. |
| RDS\_ENDPOINT\_SERVERS  S-1-5-32-576 | A group that enables member servers to run virtual machines and host sessions. |
| RDS\_MANAGEMENT\_SERVERS  S-1-5-32-577 | A group that allows members to access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). |
| HYPER\_V\_ADMINS  S-1-5-32-578 | A group that gives members access to all administrative features of Hyper-V. |
| ACCESS\_CONTROL\_ASSISTANCE\_OPS  S-1-5-32-579 | A local group that allows members to remotely query authorization attributes and permissions for resources on the local computer. |
| REMOTE\_MANAGEMENT\_USERS  S-1-5-32-580 | Members of this group can access Windows Management Instrumentation (WMI) resources over management protocols (such as WS-Management [DMTF-DSP0226]). This applies only to WMI namespaces that grant access to the user. |
| WRITE\_RESTRICTED\_CODE  S-1-5-33 | A SID that allows objects to have an ACL that lets any service process with a write-restricted token to write to the object. |
| NTLM\_AUTHENTICATION  S-1-5-64-10 | A SID that is used when the NTLM authentication package authenticated the client. |
| SCHANNEL\_AUTHENTICATION  S-1-5-64-14 | A SID that is used when the SChannel authentication package authenticated the client. |
| DIGEST\_AUTHENTICATION  S-1-5-64-21 | A SID that is used when the Digest authentication package authenticated the client. |
| THIS\_ORGANIZATION\_CERTIFICATE  S-1-5-65-1 | A SID that indicates that the client's Kerberos service ticket's PAC contained a NTLM\_SUPPLEMENTAL\_CREDENTIAL structure (as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section 2.6.4). If the OTHER\_ORGANIZATION SID is present, then this SID MUST NOT be present. [<29>](#Appendix_A_29" \o "Product behavior note 29) |
| NT\_SERVICE  S-1-5-80 | An NT Service account prefix. |
| USER\_MODE\_DRIVERS  S-1-5-84-0-0-0-0-0 | Identifies a user-mode driver process. |
| LOCAL\_ACCOUNT  S-1-5-113 | A group that includes all users who are local accounts.[<30>](#Appendix_A_30" \o "Product behavior note 30) |
| LOCAL\_ACCOUNT\_AND\_MEMBER\_OF\_ADMINISTRATORS\_GROUP  S-1-5-114 | A group that includes all users who are local accounts and members of the administrators group.[<31>](#Appendix_A_31" \o "Product behavior note 31) |
| OTHER\_ORGANIZATION  S-1-5-1000 | A group that includes all users and computers from another organization. If this SID is present, THIS\_ORGANIZATION SID MUST NOT be present.[<32>](#Appendix_A_32" \o "Product behavior note 32) |
| ALL\_APP\_PACKAGES  S-1-15-2-1 | All applications running in an app package context. |
| ML\_UNTRUSTED  S-1-16-0 | An untrusted integrity level. |
| ML\_LOW  S-1-16-4096 | A low integrity level. |
| ML\_MEDIUM  S-1-16-8192 | A medium integrity level. |
| ML\_MEDIUM\_PLUS  S-1-16-8448 | A medium-plus integrity level. |
| ML\_HIGH  S-1-16-12288 | A high integrity level. |
| ML\_SYSTEM  S-1-16-16384 | A system integrity level. |
| ML\_PROTECTED\_PROCESS  S-1-16-20480 | A protected-process integrity level. |
| ML\_SECURE\_PROCESS  S-1-16-28672 | A secure process integrity level.[<33>](#Appendix_A_33" \o "Product behavior note 33) |
| AUTHENTICATION\_AUTHORITY\_ASSERTED\_IDENTITY  S-1-18-1 | A SID that means the client's identity is asserted by an authentication authority based on proof of possession of client credentials.[<34>](#Appendix_A_34" \o "Product behavior note 34) [<35>](#Appendix_A_35" \o "Product behavior note 35) |
| SERVICE\_ASSERTED\_IDENTITY  S-1-18-2 | A SID that means the client's identity is asserted by a service.[<36>](#Appendix_A_36" \o "Product behavior note 36) [<37>](#Appendix_A_37" \o "Product behavior note 37) |
| FRESH\_PUBLIC\_KEY\_IDENTITY  S-1-18-3 | A SID that means the client's identity is asserted by an authentication authority based on proof of current possession of client public key credentials.[<38>](#Appendix_A_38" \o "Product behavior note 38) |
| KEY\_TRUST\_IDENTITY  S-1-18-4 | A SID that means the client's identity is based on proof of possession of public key credentials using the key trust object.[<39>](#Appendix_A_39" \o "Product behavior note 39) |
| KEY\_PROPERTY\_MFA  S-1-18-5 | A SID that means the key trust object had the multifactor authentication (MFA) property.[<40>](#Appendix_A_40" \o "Product behavior note 40) |
| KEY\_PROPERTY\_ATTESTATION  S-1-18-6 | A SID that means the key trust object had the attestation property.[<41>](#Appendix_A_41" \o "Product behavior note 41) |

### ACCESS\_MASK

An ACCESS\_MASK is a 32-bit set of flags that are used to encode the user rights to an object. An access mask is used both to encode the rights to an object assigned to a principal and to encode the requested access when opening an object.

The bits with an X value in the table below are used for object-specific user rights. A file object would encode, for example, Read Access and Write Access. A registry key object would encode Create Subkey and Read Value, for example.

**Note**  The bits with a value of X are reserved for use by specific protocols that make use of the ACCESS\_MASK data type. The nature of this usage differs according to each protocol and is implementation-specific.

The bits in positions 0 through 3 in the following table are generic rights that can be mapped to object-specific user rights by the [**resource manager**](#gt_a7d0361f-8608-454d-9a52-67d4d181ae09) for the requested object. The mapping of these rights is implementation-specific.

The bits with an R value in the table below are reserved.

The bits in positions 6 and 7 are for maximum allowed and access system security rights.

The bits in positions 11 through 15 are standard rights that are common to all objects.

If the **GR**/**GW**/**GX**/**GA** bits are set in an [ACE](#Section_d06e5a81176e46c69cf79137aad4455e) structure that is already attached to an object, requesting access might produce unintended results. This is because the Access Check algorithm does not map generic rights to object-specific rights for ACE structures. This mapping is only made for the requested ACCESS\_MASK passed as a parameter to the Access Check algorithm, as specified in section [2.5.3.2](#Section_4f1bbcbb814a4c70a11e2a5b8779a6f9).

1. typedef DWORD ACCESS\_MASK;
2. typedef ACCESS\_MASK\* PACCESS\_MASK;



Figure 2: Access mask bitmap table

Where the bits are defined as shown in the following table.

| Value | Description |
| --- | --- |
| **GR**  GENERIC\_READ  0x80000000L | **When used in an Access Request operation:** When read access to an object is requested, this bit is translated to a combination of bits. These are most often set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GR** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are checked against the ACE structures in the security descriptor that attached to the object.  **When used to set the Security Descriptor on an object:** When the **GR** bit is set in an ACE that is to be attached to an object, it is translated into a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GR** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are granted by this ACE. |
| **GW**  GENERIC\_WRITE  0x4000000L | **When used in an Access Request operation:** When write access to an object is requested, this bit is translated to a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GW** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are checked against the ACE structures in the security descriptor that attached to the object.  **When used to set the Security Descriptor on an object:** When the **GW** bit is set in an ACE that is to be attached to an object, it is translated into a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GW** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are granted by this ACE. |
| **GX**  GENERIC\_EXECUTE  0x20000000L | **When used in an Access Request operation:** When execute access to an object is requested, this bit is translated to a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GX** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are checked against the ACE structures in the security descriptor that attached to the object.  **When used to set the Security Descriptor on an object:** When the **GX** bit is set in an ACE that is to be attached to an object, it is translated into a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) The bits that are set are implementation dependent. During this translation, the **GX** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are granted by this ACE. |
| **GA**  GENERIC\_ALL  0x10000000L | **When used in an Access Request operation:** When all access permissions to an object are requested, this bit is translated to a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) Objects are free to include bits from the upper 16 bits in that translation as required by the objects semantics. The bits that are set are implementation dependent. During this translation, the **GA** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are checked against the ACE structures in the security descriptor that attached to the object.  **When used to set the Security Descriptor on an object:** When the **GA** bit is set in an ACE that is to be attached to an object, it is translated into a combination of bits, which are usually set in the lower 16 bits of the ACCESS\_MASK. (Individual protocol specifications MAY specify a different configuration.) Objects are free to include bits from the upper 16 bits in that translation, if required by the objects semantics. The bits that are set are implementation dependent. During this translation, the **GA** bit is cleared. The resulting ACCESS\_MASK bits are the actual permissions that are granted by this ACE. |
| MA  MAXIMUM\_ALLOWED  0x02000000L | **When used in an Access Request operation:** When requested, this bit grants the requestor the maximum permissions allowed to the object through the Access Check Algorithm. This bit can only be requested; it cannot be set in an ACE.  **When used to set the Security Descriptor on an object:** Specifying the Maximum Allowed bit in the [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) has no meaning. The MA bit SHOULD NOT be set and SHOULD be ignored when part of a SECURITY\_DESCRIPTOR structure. |
| AS  ACCESS\_SYSTEM\_SECURITY  0x01000000L | **When used in an Access Request operation:** When requested, this bit grants the requestor the right to change the SACL of an object. This bit MUST NOT be set in an ACE that is part of a DACL. When set in an ACE that is part of a SACL, this bit controls auditing of accesses to the SACL itself. |
| SY  SYNCHRONIZE  0x00100000L | Specifies access to the object sufficient to synchronize or wait on the object. |
| WO  WRITE\_OWNER  0x00080000L | Specifies access to change the owner of the object as listed in the security descriptor. |
| WD  WRITE\_DACL  0x00040000L | Specifies access to change the discretionary access control list of the security descriptor of an object. |
| RC  READ\_CONTROL  0x00020000L | Specifies access to read the security descriptor of an object. |
| DE  DELETE  0x00010000L | Specifies access to delete an object. |

### ACE

An access control entry (ACE) is used to encode the user rights afforded to a principal, either a user or group. This is generally done by combining an [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) and the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) of the principal. There are some variations to accommodate other groupings, which are specified in the following sections.

#### ACE\_HEADER

The ACE\_HEADER structure defines the type and size of an access control entry (ACE).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| AceType | | | | | | | | AceFlags | | | | | | | | AceSize | | | | | | | | | | | | | | | |

**AceType (1 byte):** An unsigned 8-bit integer that specifies the ACE types. This field MUST be one of the following values.

| Value | Meaning |
| --- | --- |
| ACCESS\_ALLOWED\_ACE\_TYPE  0x00 | Access-allowed ACE that uses the [ACCESS\_ALLOWED\_ACE (section 2.4.4.2)](#Section_72e7c7eabc024c74a619818a16bf6adb) structure. |
| ACCESS\_DENIED\_ACE\_TYPE  0x01 | Access-denied ACE that uses the [ACCESS\_DENIED\_ACE (section 2.4.4.4)](#Section_b1e1321d58164513be67b65d8ae52fe8) structure. |
| SYSTEM\_AUDIT\_ACE\_TYPE  0x02 | System-audit ACE that uses the [SYSTEM\_AUDIT\_ACE (section 2.4.4.10)](#Section_9431fd0f5b9a47f0b3f03015e2d0d4f9) structure. |
| SYSTEM\_ALARM\_ACE\_TYPE  0x03 | Reserved for future use. |
| ACCESS\_ALLOWED\_COMPOUND\_ACE\_TYPE  0x04 | Reserved for future use. |
| ACCESS\_ALLOWED\_OBJECT\_ACE\_TYPE  0x05 | Object-specific access-allowed ACE that uses the [ACCESS\_ALLOWED\_OBJECT\_ACE (section 2.4.4.3)](#Section_c79a383c2b3f4655abe7dcbb7ce0cfbe) structure.[<42>](#Appendix_A_42" \o "Product behavior note 42) |
| ACCESS\_DENIED\_OBJECT\_ACE\_TYPE  0x06 | Object-specific access-denied ACE that uses the [ACCESS\_DENIED\_OBJECT\_ACE (section 2.4.4.5)](#Section_8720fcf3865c455797b10b3489a6c270) structure.[<43>](#Appendix_A_43" \o "Product behavior note 43) |
| SYSTEM\_AUDIT\_OBJECT\_ACE\_TYPE  0x07 | Object-specific system-audit ACE that uses the [SYSTEM\_AUDIT\_OBJECT\_ACE (section 2.4.4.11)](#Section_c8da72ae6b544a0585f4e2594936d3d5) structure.[<44>](#Appendix_A_44" \o "Product behavior note 44) |
| SYSTEM\_ALARM\_OBJECT\_ACE\_TYPE  0x08 | Reserved for future use. |
| ACCESS\_ALLOWED\_CALLBACK\_ACE\_TYPE  0x09 | Access-allowed callback ACE that uses the [ACCESS\_ALLOWED\_CALLBACK\_ACE (section 2.4.4.6)](#Section_c9579cf40f4a44f19444422dfb10557a) structure.[<45>](#Appendix_A_45" \o "Product behavior note 45) |
| ACCESS\_DENIED\_CALLBACK\_ACE\_TYPE  0x0A | Access-denied callback ACE that uses the [ACCESS\_DENIED\_CALLBACK\_ACE (section 2.4.4.7)](#Section_35adad6bfda54cc1b1b59beda5b07d2e) structure.[<46>](#Appendix_A_46" \o "Product behavior note 46) |
| ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE\_TYPE  0x0B | Object-specific access-allowed callback ACE that uses the [ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE (section 2.4.4.8)](#Section_fe1838eaea344a5eb40eeb870f8322ae) structure.[<47>](#Appendix_A_47" \o "Product behavior note 47) |
| ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE\_TYPE  0x0C | Object-specific access-denied callback ACE that uses the [ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE (section 2.4.4.9)](#Section_4652f21182d54b90bd5843bf3b0fc48d) structure.[<48>](#Appendix_A_48" \o "Product behavior note 48) |
| SYSTEM\_AUDIT\_CALLBACK\_ACE\_TYPE  0x0D | System-audit callback ACE that uses the [SYSTEM\_AUDIT\_CALLBACK\_ACE (section 2.4.4.12)](#Section_bd6b6fd84bef427e9a43b9b46457e934) structure.[<49>](#Appendix_A_49" \o "Product behavior note 49) |
| SYSTEM\_ALARM\_CALLBACK\_ACE\_TYPE  0x0E | Reserved for future use. |
| SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE\_TYPE  0x0F | Object-specific system-audit callback ACE that uses the [SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE (section 2.4.4.14)](#Section_949b02e7f55d4c26969f52a009597469) structure. |
| SYSTEM\_ALARM\_CALLBACK\_OBJECT\_ACE\_TYPE  0x10 | Reserved for future use. |
| SYSTEM\_MANDATORY\_LABEL\_ACE\_TYPE  0x11 | Mandatory label ACE that uses the [SYSTEM\_MANDATORY\_LABEL\_ACE (section 2.4.4.13)](#Section_25fa65656cb046aba30a016b32c4939a) structure. |
| SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE\_TYPE  0x12 | Resource attribute ACE that uses the [SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE](#Section_352944c74fb6498880360a25dcedc730) (section 2.4.4.15) |
| SYSTEM\_SCOPED\_POLICY\_ID\_ACE\_TYPE  0x13 | A central policy ID ACE that uses the [SYSTEM\_SCOPED\_POLICY\_ID\_ACE](#Section_aa0c0f624b4c44f09718c266a6accd9f) (section 2.4.4.16) |

The term "callback" in this context does not relate to RPC call backs. [<50>](#Appendix_A_50" \o "Product behavior note 50)

**AceFlags (1 byte):** An unsigned 8-bit integer that specifies a set of ACE type-specific control flags. This field can be a combination of the following values.

| Value | Meaning |
| --- | --- |
| CONTAINER\_INHERIT\_ACE  0x02 | Child objects that are containers, such as directories, inherit the ACE as an effective ACE. The inherited ACE is inheritable unless the NO\_PROPAGATE\_INHERIT\_ACE bit flag is also set. |
| FAILED\_ACCESS\_ACE\_FLAG  0x80 | Used with system-audit ACEs in a system access control list (SACL) to generate audit messages for failed access attempts. |
| INHERIT\_ONLY\_ACE  0x08 | Indicates an inherit-only ACE, which does not control access to the object to which it is attached. If this flag is not set, the ACE is an effective ACE that controls access to the object to which it is attached.  Both effective and inherit-only ACEs can be inherited depending on the state of the other inheritance flags. |
| INHERITED\_ACE  0x10 | Indicates that the ACE was inherited. The system sets this bit when it propagates an inherited ACE to a child object.[<51>](#Appendix_A_51" \o "Product behavior note 51) |
| NO\_PROPAGATE\_INHERIT\_ACE  0x04 | If the ACE is inherited by a child object, the system clears the OBJECT\_INHERIT\_ACE and CONTAINER\_INHERIT\_ACE flags in the inherited ACE. This prevents the ACE from being inherited by subsequent generations of objects. |
| OBJECT\_INHERIT\_ACE  0x01 | Noncontainer child objects inherit the ACE as an effective ACE.  For child objects that are containers, the ACE is inherited as an inherit-only ACE unless the NO\_PROPAGATE\_INHERIT\_ACE bit flag is also set. |
| SUCCESSFUL\_ACCESS\_ACE\_FLAG  0x40 | Used with system-audit ACEs in a SACL to generate audit messages for successful access attempts. |

**AceSize (2 bytes):** An unsigned 16-bit integer that specifies the size, in bytes, of the ACE. The **AceSize** field can be greater than the sum of the individual fields, but MUST be a multiple of 4 to ensure alignment on a [DWORD](#Section_262627d83418462792184ffe110850b2) boundary. In cases where the **AceSize** field encompasses additional data for the callback ACEs types, that data is implementation-specific. Otherwise, this additional data is not interpreted and MUST be ignored.

##### ACE\_HEADER--RPC representation

The RPC representation of the [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) defines the type and size of an [ACE](#Section_d06e5a81176e46c69cf79137aad4455e). The members and values are as specified in section 2.4.4.1.

1. typedef struct \_ACE\_HEADER {
2. UCHAR AceType;
3. UCHAR AceFlags;
4. USHORT AceSize;
5. } ACE\_HEADER,
6. \*PACE\_HEADER;

#### ACCESS\_ALLOWED\_ACE

The ACCESS\_ALLOWED\_ACE structure defines an ACE for the discretionary access control list (DACL) that controls access to an object. An access-allowed ACE allows access to an object for a specific trustee identified by a security identifier (SID).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights allowed by this ACE.

**Sid (variable):** The [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) of a trustee. The length of the SID MUST be a multiple of 4.

#### ACCESS\_ALLOWED\_OBJECT\_ACE

The ACCESS\_ALLOWED\_OBJECT\_ACE structure defines an ACE that controls allowed access to an object, a property set, or property. The ACE contains a set of access rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object, and a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies the trustee to whom the system will grant access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights allowed by this ACE.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_DELETE\_CHILD  0X00000002 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to delete this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** are valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, property, extended right, or type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE \_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored. For information on access rights and for a mapping of the control access rights to the corresponding GUID value that identifies each right, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) sections 5.1.3.2 and 5.1.3.2.1.

ACCESS\_MASK bits are not mutually exclusive. Therefore, the **ObjectType** field can be set in an [ACE](#Section_d06e5a81176e46c69cf79137aad4455e) with any ACCESS\_MASK. If the AccessCheck algorithm calls this ACE and does not find an appropriate GUID, then that ACE will be ignored. For more information on access checks and object access, see [MS-ADTS] section 5.1.3.3.3.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

#### ACCESS\_DENIED\_ACE

The ACCESS\_DENIED\_ACE structure defines an ACE for the DACL that controls access to an object. An access-denied ACE denies access to an object for a specific trustee identified by a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights denied by this ACE.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

#### ACCESS\_DENIED\_OBJECT\_ACE

The ACCESS\_DENIED\_OBJECT\_ACE structure defines an ACE that controls denied access to an object, a property set, or a property. The ACE contains a set of access rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object, and a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies the trustee to whom the system will deny access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights allowed by this ACE.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_DELETE\_CHILD  0X00000002 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to delete this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** is valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, a property, an extended right, or a type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE \_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored. For information about access rights and for a mapping of the control access rights to the corresponding GUID value that identifies each right, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) sections 5.1.3.2 and 5.1.3.2.1.

ACCESS\_MASK bits are not mutually exclusive. Therefore, the **ObjectType** field can be set in an [ACE](#Section_d06e5a81176e46c69cf79137aad4455e) with any ACCESS\_MASK. If the AccessCheck algorithm calls this ACE and does not find an appropriate GUID, that ACE will be ignored. For more information about access checks and object access, see [MS-ADTS] section 5.1.3.3.3.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

#### ACCESS\_ALLOWED\_CALLBACK\_ACE

The ACCESS\_ALLOWED\_CALLBACK\_ACE structure defines an ACE for the DACL that controls access to an object. An access-allowed ACE allows access to an object for a specific trustee identified by a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights allowed by this ACE.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### ACCESS\_DENIED\_CALLBACK\_ACE

The ACCESS\_DENIED\_CALLBACK\_ACE structure defines an ACE for the DACL that controls access to an object. An access-denied ACE denies access to an object for a specific trustee identified by a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that specifies the user rights denied by this ACE.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE

The ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE structure defines an ACE that controls allowed access to an object, property set, or property. The ACE contains a set of user rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object, and a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies the trustee to whom the system will grant access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights allowed by this ACE.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** are valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, property, extended right, or type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE \_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE

The ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE structure defines an ACE that controls denied access to an object, a property set, or property. The ACE contains a set of user rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object, and a [SID](#Section_f992ad600fe44b879fedbeb478836861) that identifies the trustee to whom the system will deny access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights denied by this ACE.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** are valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, property, extended right, or type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE \_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### SYSTEM\_AUDIT\_ACE

The SYSTEM\_AUDIT\_ACE structure defines an access ACE for the system access control list (SACL) that specifies what types of access cause system-level notifications. A system-audit ACE causes an audit message to be logged when a specified trustee attempts to gain access to an object. The trustee is identified by a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights that cause audit messages to be generated.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4. An access attempt of a kind specified by the **Mask** field by any trustee whose SID matches the **Sid** field causes the system to generate an audit message. If an application does not specify a SID for this field, audit messages are generated for the specified access rights for all trustees.

#### SYSTEM\_AUDIT\_OBJECT\_ACE

The [SYSTEM\_AUDIT\_OBJECT\_ACE](#Section_949b02e7f55d4c26969f52a009597469) structure defines an ACE for a SACL. The ACE can audit access to an object or subobjects, such as property sets or properties. The ACE contains a set of user rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object or subobject, and a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies the trustee for whom the system will audit access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights that cause audit messages to be generated.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** is valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, a property, an extended right, or a type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE\_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### SYSTEM\_AUDIT\_CALLBACK\_ACE

The SYSTEM\_AUDIT\_CALLBACK\_ACE structure defines an ACE for the SACL that specifies what types of access cause system-level notifications. A system-audit ACE causes an audit message to be logged when a specified trustee attempts to gain access to an object. The trustee is identified by a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights that cause audit messages to be generated.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4. An access attempt of a kind specified by the **Mask** field by any trustee whose SID matches the **Sid** field causes the system to generate an audit message. If an application does not specify a SID for this field, audit messages are generated for the specified access rights for all trustees.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### SYSTEM\_MANDATORY\_LABEL\_ACE

The SYSTEM\_MANDATORY\_LABEL\_ACE structure defines an ACE for the SACL that specifies the mandatory access level and policy for a securable object.[<52>](#Appendix_A_52" \o "Product behavior note 52)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the access policy for principals with a mandatory integrity level lower than the object associated with the SACL that contains this ACE.

| Value | Meaning |
| --- | --- |
| SYSTEM\_MANDATORY\_LABEL\_NO\_WRITE\_UP  0x00000001 | A principal with a lower mandatory level than the object cannot write to the object. |
| SYSTEM\_MANDATORY\_LABEL\_NO\_READ\_UP  0x00000002 | A principal with a lower mandatory level than the object cannot read the object. |
| SYSTEM\_MANDATORY\_LABEL\_NO\_EXECUTE\_UP  0x00000004 | A principal with a lower mandatory level than the object cannot execute the object. |

**Sid (variable):** The [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) of a trustee. The length of the SID MUST be a multiple of 4. The identifier authority of the SID must be SECURITY\_MANDATORY\_LABEL\_AUTHORITY. The RID of the SID specifies the mandatory integrity level of the object associated with the SACL that contains this ACE. The RID must be one of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Untrusted integrity level. |
| 0x00001000 | Low integrity level. |
| 0x00002000 | Medium integrity level. |
| 0x00003000 | High integrity level. |
| 0x00004000 | System integrity level. |
| 0x00005000 | Protected process integrity level. |

##### SYSTEM\_MANDATORY\_LABEL\_ACE--RPC Representation

The RPC representation of the [SYSTEM\_MANDATORY\_LABEL\_ACE](#Section_25fa65656cb046aba30a016b32c4939a) type defines an [access control entry (ACE)](#Section_d06e5a81176e46c69cf79137aad4455e) for the [**system access control list (SACL)**](#gt_c189801e-3752-4715-88f4-17804dad5782) that specifies the mandatory access level and policy for a securable object.

1. typedef struct \_SYSTEM\_MANDATORY\_LABEL\_ACE {
2. ACE\_HEADER Header;
3. ACCESS\_MASK Mask;
4. DWORD SidStart;
5. } SYSTEM\_MANDATORY\_LABEL\_ACE,
6. \*PSYSTEM\_MANDATORY\_LABEL\_ACE;

**Header:**  An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure, as specified in section 2.4.4.13.

**Mask:**  An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) as specified in section 2.4.4.13.

**SidStart:**  Specifies the first [DWORD](#Section_262627d83418462792184ffe110850b2) of the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25). The remaining bytes of the SID are stored in contiguous memory after the **SidStart** member. The **IdentifierAuthority** and **RID** MUST be as specified 2.4.4.13.

#### SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE

The SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE structure defines an ACE for a SACL. The ACE can audit access to an object or subobjects, such as property sets or properties. The ACE contains a set of user rights, a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the type of object or subobject, and a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies the trustee for whom the system will audit access. The ACE also contains a GUID and a set of flags that control inheritance of the ACE by child objects.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| InheritedObjectType (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ApplicationData (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It contains flags that control inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) structure that specifies the user rights that cause audit messages to be generated.

| Value | Meaning |
| --- | --- |
| ADS\_RIGHT\_DS\_CONTROL\_ACCESS  0X00000100 | The **ObjectType** GUID identifies an extended access right. |
| ADS\_RIGHT\_DS\_CREATE\_CHILD  0X00000001 | The **ObjectType** GUID identifies a type of child object. The ACE controls the trustee's right to create this type of child object. |
| ADS\_RIGHT\_DS\_READ\_PROP  0x00000010 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to read the property or property set. |
| ADS\_RIGHT\_DS\_WRITE\_PROP  0x00000020 | The **ObjectType** GUID identifies a property set or property of the object. The ACE controls the trustee's right to write the property or property set. |
| ADS\_RIGHT\_DS\_SELF  0x00000008 | The **ObjectType** GUID identifies a validated write. |

**Flags (4 bytes):** A 32-bit unsigned integer that specifies a set of bit flags that indicate whether the **ObjectType** and **InheritedObjectType** fields contain valid data. This parameter can be one or more of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Neither **ObjectType** nor **InheritedObjectType** are valid. |
| ACE\_OBJECT\_TYPE\_PRESENT  0x00000001 | **ObjectType** is valid. |
| ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT  0x00000002 | **InheritedObjectType** is valid. If this value is not specified, all types of child objects can inherit the ACE. |

**ObjectType (16 bytes):** A GUID that identifies a property set, property, extended right, or type of child object. The purpose of this GUID depends on the user rights specified in the **Mask** field. This field is valid only if the ACE\_OBJECT\_TYPE\_PRESENT bit is set in the **Flags** field. Otherwise, the **ObjectType** field is ignored.

**InheritedObjectType (16 bytes):** A GUID that identifies the type of child object that can inherit the ACE. Inheritance is also controlled by the inheritance flags in the ACE\_HEADER, as well as by any protection against inheritance placed on the child objects. This field is valid only if the ACE\_INHERITED\_OBJECT\_TYPE\_PRESENT bit is set in the Flags member. Otherwise, the **InheritedObjectType** field is ignored.

**Sid (variable):** The SID of a trustee. The length of the SID MUST be a multiple of 4.

**ApplicationData (variable):** Optional application data. The size of the application data is determined by the **AceSize** field of the ACE\_HEADER.

#### SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE

The SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE structure defines an ACE for the specification of a resource attribute associated with an object. A SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE is used in conditional ACEs in specifying access or audit policy for the resource.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Attribute Data (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of the ACE. It also contains flags that control applicability and inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that MUST be set to zero.

**Sid (variable):** The [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) corresponding to the Everyone SID (S-1-1-0) in binary form.

**Attribute Data (variable):** Data describing a resource attribute type, name, and value(s). This data MUST be encoded in [CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#Section_21f2b5f0737645bbbc31eaa60841dbe9) format as described in section 2.4.10.1

#### SYSTEM\_SCOPED\_POLICY\_ID\_ACE

The SYSTEM\_SCOPED\_POLICY\_ID\_ACE structure defines an ACE for the purpose of applying a central access policy to the resource.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Header | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mask | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Header (4 bytes):** An [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586) structure that specifies the size and type of ACE. It also contains flags that control applicability and inheritance of the ACE by child objects.

**Mask (4 bytes):** An [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) that MUST be set to zero.

**Sid (variable):** A [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that identifies a central access policy. For a SYSTEM\_SCOPED\_POLICY\_ID\_ACE to be applicable on a resource, this SID MUST match a **CAPID** of a CentralAccessPolicy contained in the **CentralAccessPoliciesList** (as specified in [[MS-GPCAP]](%5bMS-GPCAP%5d.pdf#Section_5189d5c912c2491cbf16f7008c46c6fb) section 3.2.1.1) of the machine on which the access evaluation will be performed.

#### Conditional ACEs

Conditional ACEs are a form of CALLBACK ACEs with a special format of the application data. A Conditional ACE allows a conditional expression to be evaluated when an access check (as specified in section [2.5.3.2](#Section_4f1bbcbb814a4c70a11e2a5b8779a6f9)) is performed.[<53>](#Appendix_A_53" \o "Product behavior note 53)

The following ACE types can be formatted as a Conditional ACE:

* [ACCESS\_ALLOWED\_CALLBACK\_ACE](#Section_c9579cf40f4a44f19444422dfb10557a)
* [ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE](#Section_fe1838eaea344a5eb40eeb870f8322ae)
* [ACCESS\_DENIED\_CALLBACK\_ACE](#Section_35adad6bfda54cc1b1b59beda5b07d2e)
* [ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE](#Section_4652f21182d54b90bd5843bf3b0fc48d)
* [SYSTEM\_AUDIT\_CALLBACK\_ACE](#Section_bd6b6fd84bef427e9a43b9b46457e934)
* [SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE](#Section_949b02e7f55d4c26969f52a009597469)

A Conditional ACE is a CALLBACK ACE in which the first four bytes of the **ApplicationData** field in the CALLBACK ACE structure are set to the following byte value sequence: 0x61 0x72 0x74 0x78. The remaining contents of the **ApplicationData** field specify a conditional expression. The conditional expression language constructs and binary representation are defined in this section.

The security descriptor definition language (SDDL) (section [2.5.1](#Section_4f4251cc23b644b693ba69688422cb06)) provides syntax for defining conditional ACEs in a string format in section [2.5.1.1](#Section_f4296d691c0f491f9587a960b292d070).

##### Conditional ACE Expressions

This section defines the semantics and format of the ApplicationData field of a callback ACE holding a conditional expression.

Conditional expressions are logical expressions that are part of a conditional ACE (section [2.4.4.17](#Section_10dc22eb788d4343b5560b6969fe58ca)) and are evaluated during an access check evaluation to determine if the effect (to allow or deny the specified permissions) of the conditional ACE is to apply in the access check valuation.

A conditional expression is composed of a series of one or more simpler conditional expressions or expression terms in syntactical relation to logical operators and security attributes such that when evaluated, the expression will produce TRUE, FALSE, or UNKNOWN. Conditional expressions can be operands to the AND, OR, or NOT logical operators. (Logical operators are defined in section [2.4.4.17.7](#Section_6e92a8b360d84cc08441dd6ba6e59e63).)

##### Security Attributes

Conditional expression terms contain references to security attributes (also known as claims) of an authenticated principal or a resource. Security attributes that are associated with authenticated user principal and device principal entities are referred to as "user claims" and "device claims", respectively, and are defined as an instance of a CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure associated with a token/authorization context. User claims are associated with the UserClaims[] array, and device claims are associated with the DeviceClaims[] array as described in section [2.5.2](#Section_efc83c3252754dffa3e2973c9624711b). An attribute associated with a resource is referred to as a "resource attribute" and is defined as a [CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#Section_21f2b5f0737645bbbc31eaa60841dbe9) (section 2.4.10.1) structure within a [SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE](#Section_352944c74fb6498880360a25dcedc730) contained in the Security Descriptor SACL associated with a resource.

##### Conditional ACE Applicability

If the result evaluation of the conditional expression is FALSE, then the corresponding conditional ACE does not apply in the access check evaluation.

If the result of evaluation of the conditional expression is TRUE, then the conditional ACE applies in the access check evaluation. If the conditional ACE is an ACCESS\_ALLOWED\_CALLBACK\_ACE type and the ACE applies, then the permissions in the **Mask** member of the **ACE\_HEADER** structure are granted. If the conditional ACE is an ACCESS\_DENIED\_CALLBACK\_ACE and the ACE applies, then the permissions are denied in the access check evaluation.

If the result of the evaluation of the conditional expression is UNKNOWN and the conditional ACE is an ACCESS\_ALLOWED\_CALLBACK\_ACE type, then the permissions in the **Mask** member variable are not granted by this ACE in the access check evaluation.

If the result of the evaluation of the conditional expression is UNKNOWN and the conditional ACE is an ACCESS\_DENIED\_CALLBACK\_ACE type, then the permissions in the **Mask** member variable are denied in the access check evaluation.

##### Conditional ACE Binary Formats

Conditional expressions are stored in the **ApplicationData** member of certain CALLBACK ACE types (section [2.4.4.17](#Section_10dc22eb788d4343b5560b6969fe58ca)) where each operator ID and operand is persisted in postfix notation.

A CALLBACK ACE contains a conditional expression if the **ApplicationData** member is prefixed by 0x61, 0x72, 0x74, 0x78 (the ACE\_CONDITION\_SIGNATURE) and the remainder of the data in the **ApplicationData** member immediately following the conditional ACE signature specifies a conditional expression (section [2.4.4.17.1](#Section_fedb7cc4180b4e0b9b95fba8a6c8402b)).

Conditional expressions are encoded in contiguous memory as a series of tokens. The first byte of each token must be a byte-code identifying the token type. The token type determines the format of the token in memory. Tokens take one of three formats:

1. Operator: A single byte-code, which identifies a logical or relational operator.
2. Literal: A token byte-code that identifies a built-in data type and implies a token type of "literal", followed by the encoded representation of the literal. Literal tokens can be single values or multivalued. A multivalued literal is encoded as a composite byte-code followed by each contained literal value.
3. Attribute Name: A byte-code identifying an attribute type and name.

The following tables provide the set of valid tokens and each token's syntax. The first byte of a token is the byte-code and the remainder of the token is the token-data and is formatted according the token's syntax. All multibyte integers, including any Unicode characters, MUST be stored least-significant byte (LSB) first.

Conditional expressions are at the end of the ACE in contiguous memory; the ending of the ACEs MUST align on a [DWORD](#Section_262627d83418462792184ffe110850b2) boundary. Any additional bytes needed to achieve DWORD boundary alignment MUST be set to 0x00.

For tokens representing literal values, the base and sign MUST be specified from the possible values specified in the following tables.

##### Literal Tokens

| Token Type | Byte-Code | Token Data Encoding |
| --- | --- | --- |
| Invalid token | 0x00 | Padding value. |
| Signed int8 | 0x01 | 1 [QWORD](#Section_ac050bbfa8214fabbccfd95d892f428f), least significant byte first, for the value, 2's complement, -128 to +127.  1 [BYTE](#Section_d7edc080e4994219a8371bc40b64bb04) for sign. (possible values for sign in the following table) .  1 BYTE for base. (possible values for base in the following table). |
| Signed int16 | 0x02 | 1 QWORD, least significant byte first, 2's complement, -32768 to +32767.  1 BYTE for sign.  1 BYTE for base. |
| Signed int32 | 0x03 | 1 QWORD, least significant byte first, 2's complement.  1 BYTE for sign.  1 BYTE for base. |
| Signed int64 | 0x04 | 1 QWORD, least significant byte first, 2's complement.  1 BYTE for sign.  1 BYTE for base. |
| Unicode String | 0x10 | 1 [DWORD](#Section_262627d83418462792184ffe110850b2) for the length in bytes.  1 [WORD](#Section_f8573df3a44a4a50b070ac4c3aa78e3c) for each Unicode character. Characters are stored LSB first. Strings are not null-terminated. |
| Octet String | 0x18 | Custom data is represented as a contiguous sequence of bytes.  1 DWORD for the length in bytes.  1 BYTE for each data octet. |
| Composite | 0x50 | 1 DWORD that specifies the entire length in bytes of the entire set of elements.  List type--can be heterogeneous. Elements are stored in contiguous fashion according to the built-in data type storage rules. |
| SID | 0x51 | 1 DWORD that specifies the entire length in bytes of the SID.  SID in binary representation (as specified in section [2.4.2.2](#Section_f992ad600fe44b879fedbeb478836861).) |

Tokens in the preceding table that contain a base MUST include a base code from the following table.

| Base | Code | Description |
| --- | --- | --- |
| 8 | 0x01 | Octal |
| 10 | 0x02 | Decimal |
| 16 | 0x03 | Hexadecimal |

Tokens in the preceding table that contain signs MUST include a sign code from the following table.

Relational operators interpret no sign (0x03) as positive.

Relational operators MUST use this to determine the sign of the literal during evaluation.

| Sign | Code | Description |
| --- | --- | --- |
| + | 0x01 | Plus sign in condition. |
| - | 0x02 | Minus sign in condition. |
| None | 0x03 | No sign in condition. |

Thus the decimal value -1 encoded as a signed int64 would have the following binary representation (byte code, QWORD, sign byte, base byte):

1. 0x04 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x02 0x02

##### Relational Operator Tokens

Each relational operator examines one or more attribute values and evaluates to TRUE, FALSE or UNKNOWN, according to the defined behavior of the operator in the following table. In addition to the TRUE and FALSE values specified for each operator in the table, each relational operator MUST return "UNKNOWN" if the attribute tested does not exist in the security context.

For all operators other than the relational operators ==, Contains, and Any\_of, and the logical operator Exists, when multivalued attributes are on the left- and/or right-hand side of an operator, the operation will fail and produce an UNKNOWN value.

If any processing rule returns an error, then the entire conditional expression evaluates to UNKNOWN, regardless of the rest of the expression.

**Unary Relational Operators:**

The operand type MUST be either a [SID](#Section_f992ad600fe44b879fedbeb478836861) literal, or a composite, each of whose elements is a SID literal.

The operand for unary operators is the variable on the top of the evaluation stack as specified in the [EvaluateAceCondition](#Section_bb4ad6b36a114b2db5b0b17456147c46) algorithm in section 2.5.3.1.5.

| Token Type | Byte-Code | Processing |
| --- | --- | --- |
| Member\_of | 0x89 | SDDL Form: **Member\_of** *operand*  Return TRUE if **SIDs[]** array (section [2.5.2](#Section_efc83c3252754dffa3e2973c9624711b)) contains all of the SIDs in the operand; FALSE otherwise. |
| Device\_Member\_of[<54>](#Appendix_A_54" \o "Product behavior note 54) | 0x8a | SDDL Form: **Device\_Member\_of** *operand*  Return TRUE if **DeviceSIDs[]** array (section 2.5.2) contains all of the SIDs in the operand; FALSE otherwise. |
| Member\_of\_Any[<55>](#Appendix_A_55" \o "Product behavior note 55) | 0x8b | SDDL Form: **Member\_of\_Any** *operand*  Return TRUE if **SIDs[]** array (section 2.5.2) contains any of the SIDs in the operand; FALSE otherwise. |
| Device\_Member\_of\_Any[<56>](#Appendix_A_56" \o "Product behavior note 56) | 0x8c | SDDL Form: **Device\_Member\_of\_Any** *operand*  Return TRUE if **DeviceSIDs[]** array (section 2.5.2) contains any of the SIDs in the operand; FALSE otherwise. |
| Not\_Member\_of[<57>](#Appendix_A_57" \o "Product behavior note 57) | 0x90 | SDDL Form: **Not\_Member\_of** *operand*  Logical inverse of **Member\_of**. |
| Not\_Device\_Member\_of[<58>](#Appendix_A_58" \o "Product behavior note 58) | 0x91 | SDDL Form: **Not\_Device\_Member\_of** *operand*  Logical inverse of **Device\_Member\_of**. |
| Not\_Member\_of\_Any[<59>](#Appendix_A_59" \o "Product behavior note 59) | 0x92 | SDDL Form: **Not\_Member\_of\_Any** *operand*  Logical inverse of **Not\_Member\_of\_Any**. |
| Not\_Device\_Member\_of\_Any[<60>](#Appendix_A_60" \o "Product behavior note 60) | 0x93 | SDDL Form: **Not\_Device\_Member\_of\_Any** *operand*  Logical inverse of **Device\_Member\_of\_Any**. |

**Binary Relational Operators**

Binary relational operators compare left-hand-side (LHS) and right-hand-side (RHS) operands. The LHS MUST contain an attribute name in simple or @Prefixed form.[<61>](#Appendix_A_61" \o "Product behavior note 61) The RHS MUST contain an attribute in @Prefixed form or literals representing values of the same value type as the attribute variable on the LHS. If the LHS and RHS operands are of different types, then the entire conditional expression evaluates to UNKNOWN. Note, however, that BOOLEAN values TRUE and FALSE can be compared to the literal integers "1" and "0", but only when using the == or != operators.

Relational operators that compare string and octet string values compare each string operand byte by byte, terminating when the compared bytes differ in value. If a string is a prefix of a string it is compared to, the longer string is considered greater. The comparison is case-insensitive, unless the CLAIM\_SECURITY\_ATTRIBUTE\_VALUE\_CASE\_SENSITIVE flag value is set in the [CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#Section_21f2b5f0737645bbbc31eaa60841dbe9) structure (section 2.4.10.1).[<62>](#Appendix_A_62" \o "Product behavior note 62)

If the type of an operand is "Result Value" then the operation returns an error.

If the type of an operand is "Local Attribute", "Resource Attribute", "Device Attribute" or "User Attribute" and the value is null then the logical value of the operand is UNKNOWN.

If the value of either operand is UNKNOWN then the operation returns UNKNOWN.

In the following processing rules, the LHS is the second variable on the stack and the RHS is the top of the stack as specified in the EvaluateAceCondition algorithm in section 2.5.3.1.5.

| Token Type | Byte-Code | Processing |
| --- | --- | --- |
| == | 0x80 | SDDL form: (*LHS == RHS*)  MUST evaluate to TRUE if the argument on the RHS evaluates to the exact value (single or set value) of the argument on the LHS; otherwise, FALSE. |
| != | 0x81 | SDDL form: (*LHS != RHS*)  MUST evaluate to FALSE if the argument on the RHS evaluates to the exact value of the argument on LHS; otherwise, TRUE. |
| < | 0x82 | SDDL form: (*LHS < RHS*)  MUST evaluate to TRUE if the argument on the LHS is less than the argument on the RHS; otherwise, FALSE. |
| <= | 0x83 | SDDL form: (*LHS <= RHS*)  MUST evaluate to TRUE if the argument on the LHS is less than, or equal to, the argument on the RHS; otherwise, FALSE. |
| > | 0x84 | SDDL form: (*LHS > RHS*)  MUST evaluate to TRUE if the argument on the LHS is greater than the argument on the RHS; otherwise, FALSE. |
| >= | 0x85 | SDDL form: (*LHS >= RHS*)  MUST evaluate to TRUE if the argument on the LHS is greater than, or equal to, the argument on the RHS; otherwise, FALSE. |
| Contains | 0x86 | SDDL Form: *LHS* **Contains** *RHS*  LHS MUST be an attribute name in simple or @Prefixed form.  RHS MUST be a set of one or more literals, or an attribute name in @Prefixed form.  MUST evaluate to TRUE if the value(s) for the specified LHS includes value(s) identical to each of the value(s) specified by the RHS; otherwise, FALSE.[<63>](#Appendix_A_63" \o "Product behavior note 63) |
| Any\_of | 0x88 | SDDL Form: *LHS* **Any\_of** *RHS*  LHS MUST be an attribute name in simple or @Prefixed form. RHS MUST be a set of one or more literals, or an attribute name in @Prefixed form.  MUST evaluate to TRUE if the RHS value set includes one or more of the value(s) of the specified LHS; otherwise, FALSE. RHS can be either a set or a single value.[<64>](#Appendix_A_64" \o "Product behavior note 64) |
| Not\_Contains[<65>](#Appendix_A_65" \o "Product behavior note 65) | 0x8e | SDDL Form: *LHS* **Not\_Contains** *RHS*  Logical inverse of **Contains**. |
| Not\_Any\_of[<66>](#Appendix_A_66" \o "Product behavior note 66) | 0x8f | Form: *LHS* **Not\_Any\_of** RHS  Logical inverse of **Any\_of**. |

##### Logical Operator Tokens

Logical operators test the logical value of operands and produce TRUE, FALSE, or UNKNOWN according to the defined behavior of the operator. The operands of logical operators must be conditional expressions and/or expression terms. The logical value of an operand is the tri-state logical value it receives when evaluated according to the following:

* If the type of the operand is "Literal" then the operation returns an error.
* If the type of the operand is "Local Attribute", "Resource Attribute", "Device Attribute" or "User Attribute" and the value is null then the logical value of the operand is UNKNOWN.
* If an operand is a "Local Attribute", "Resource Attribute", "Device Attribute" or "User Attribute" and the value is an integer, the logical value of the operand is TRUE if the value is nonzero, and FALSE otherwise.
* If an operand is a "Local Attribute", "Resource Attribute", "Device Attribute" or "User Attribute" and the value is string, the logical value of the operand is TRUE if the length of the string is nonzero, and FALSE otherwise.
* If the type of an operand is "Result Value", the logical value of the operand is the value of the operand.
* If any processing rule returns an error, then the entire conditional expression evaluates to UNKNOWN regardless of the rest of the expression.

**Unary Logical Operators**

The operand for unary operators is the variable on the top of the evaluation stack as specified in the EvaluateAceCondition algorithm in section [2.5.3.1.5](#Section_bb4ad6b36a114b2db5b0b17456147c46).

| Token Type | Byte-Code | Processing |
| --- | --- | --- |
| Exists | 0x87 | SDDL Form: **Exists** *operand*   1. If the type of the operand is "Local Attribute" 2. If the value is non-null return TRUE 3. Else return FALSE 4. Else if the type of the operand is "Resource Attribute" 5. Return TRUE if value is non-null; FALSE otherwise. 6. Else return Error |
| Not\_Exists[<67>](#Appendix_A_67" \o "Product behavior note 67) | 0x8d | SDDL Form: **Not\_Exists** *operand*  Logical inverse of **Exists**. |
| Logical NOT (!) | 0xa2 | 1. If the logical value of the operand is TRUE 2. Return FALSE 3. If the logical value of the operand is FALSE 4. Return TRUE 5. If the logical value of the operand is UNKNOWN 6. Return UNKNOWN |

**Binary Logical Operators**

In the processing rules that follow, the LHS is the second element on the stack and the RHS is the top of the stack as specified in the EvaluateAceCondition algorithm in section 2.5.3.1.5.

| Token Type | Byte-Code | Processing |
| --- | --- | --- |
| logical AND (&&) | 0xa0 | SDDL Form: *LHS* **&&** *RHS*   1. If the logical value of either operand is FALSE 2. Return FALSE 3. Else if the logical value of either operand is UNKNOWN 4. Return UNKNOWN 5. Else Return TRUE |
| logical OR (||) | 0xa1 | SDDL Form: *LHS* **||** *RHS*   1. If the logical value of either operand is TRUE 2. Return TRUE 3. Else if the logical value of either operand is UNKNOWN 4. Return UNKNOWN 5. Else Return FALSE |

##### Attribute Tokens

Attributes can be associated with local environments, users, resources, or devices.

| Token Type | Byte-Code | Token Data Encoding |
| --- | --- | --- |
| Local Attribute | 0xf8 | Encoding same as Unicode string.  Lookup based on string name. |
| User Attribute | 0xf9 | Encoding same as Unicode String.  Lookup based on string name. |
| Resource Attribute | 0xfa | Encoding same as Unicode String.  Lookup based on string name. |
| Device Attribute | 0xfb | Encoding same as Unicode String.  Lookup based on string name. |

##### Examples: Conditional Expression Binary Representation

**Example 1: Attributes in Simple Form**

For the following conditional expression:

1. (Title=="VP")

The **ApplicationData** member of the CALLBACK ACEs structure will have the following physical packing (numbers are in hexadecimal):

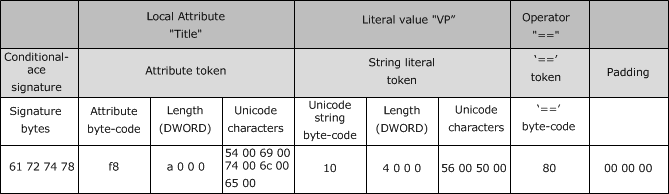


Figure 3: Components of the Application Data member for the conditional expression (Title=="VP")

The following hexadecimal byte dump shows the contents of the ApplicationData in contiguous memory for the preceding conditional expression (with three added bytes for padding).

1. 61 72 74 78 f8 0a 00 00 artx....
2. 00 54 00 69 00 74 00 6c .T.i.t.l
3. 00 65 00 10 04 00 00 00 .e......
4. 56 00 50 00 80 00 00 00 V.P.....

**Example 2: @Prefixed Attribute Names and Multiple Terms**

For the following conditional expression illustrates @Prefixed attribute names and use of multiple terms as expressed in SDDL:

1. (@User.smartcard==1 || @Device.managed==1) && (@Resource.dept Any\_of{"Sales","HR"})

SDDL strings encoded into an ApplicationData field MUST be ordered to maintain SDDL precedence rules as specified in section [2.5.1.3](#Section_d1a8392f3f544fea823344ede9eb198c). The preceding conditional expression expressions can be reordered in postfix notation as follows:

| @User.smartcard | 1 | == | @Device.managed | 1 | == | || | @Resource.dept | {Sales,HR} | Any\_of | && |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

The following figure shows the mapping from the above postfix expression to the layout in memory:

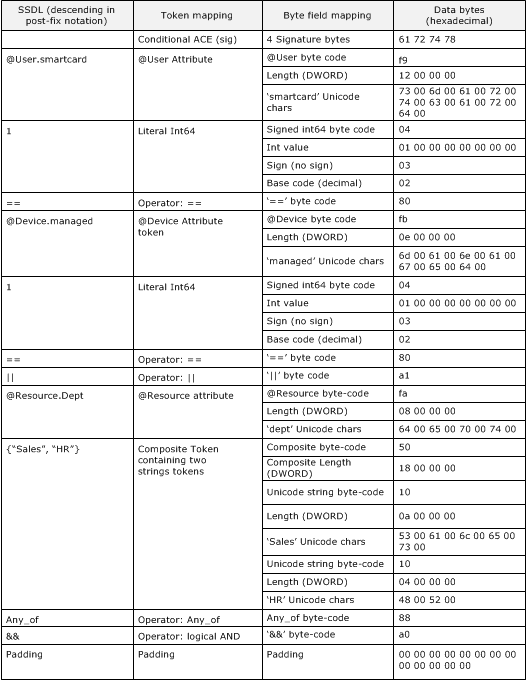


Figure 4: Postfix to memory mapping for "(@User.smartcard == 1 || @Device.managed == 1) && (@Resource.dept Any\_of {"Sales","HR"})"

**Example 3: RHS Attribute Variables and SID-based Operators**

The following conditional expression illustrates @Prefixed attribute names with an attribute variable on the RHS of the operator and the use of a SID-based operator (Member\_Of) as expressed in SDDL:

1. (@User.clearanceLevel>=@Resource.requiredClearance) || (Member\_of{SID(BA)})

SDDL strings encoded into an **ApplicationData** field MUST be ordered to maintain SDDL precedence rules as specified in section 2.5.1.3. The preceding conditional expression can be reordered in postfix notation as follows:

| @User.clearanceLevel | @Resource.requiredClearance | >= | {SID(BA)} | Member\_of | || |
| --- | --- | --- | --- | --- | --- |

The following figure shows the mapping from the preceding postfix expression to the layout in memory.

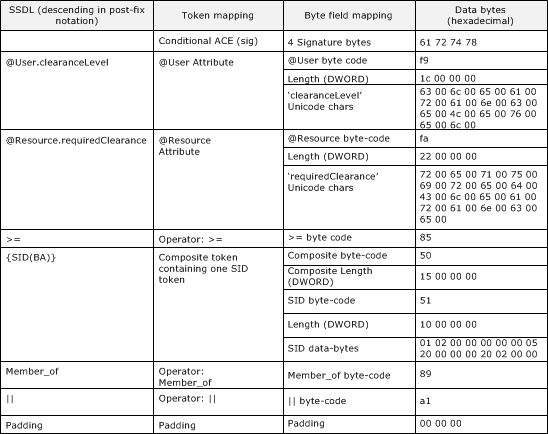


Figure 5: Postfix to memory mapping for (@User.clearanceLevel >= @Resource.requiredClearance) || (Member\_of {SID(BA)})

### ACL

The access control list (ACL) packet is used to specify a list of individual access control entries ([ACEs](#Section_d06e5a81176e46c69cf79137aad4455e)). An ACL packet and an array of ACEs comprise a complete access control list.

The individual ACEs in an ACL are numbered from 0 to n, where n+1 is the number of ACEs in the ACL. When editing an ACL, an application refers to an ACE within the ACL by the ACE index.

In the absence of implementation-specific functions to access the individual ACEs, access to each ACE MUST be computed by using the **AclSize** and **AceCount** fields to parse the wire packets following the ACL to identify each [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586), which in turn contains the information needed to obtain the specific ACEs.

An ACL is said to be in canonical form if:

* All explicit ACEs are placed before inherited ACEs.
* Within the explicit ACEs, deny ACEs come before grant ACEs.
* Deny ACEs on the object come before deny ACEs on a child or property.
* Grant ACEs on the object come before grant ACEs on a child or property.
* Inherited ACEs are placed in the order in which they were inherited.

There are two types of ACL:

* A [**discretionary access control list (DACL)**](#gt_d727f612-7a45-48e4-9d87-71735d62b321) is controlled by the owner of an object or anyone granted WRITE\_DAC access to the object. It specifies the access particular users and groups can have to an object. For example, the owner of a file can use a DACL to control which users and groups can and cannot have access to the file.
* A [**system access control list (SACL)**](#gt_c189801e-3752-4715-88f4-17804dad5782) is similar to the DACL, except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log. Each ACE in a SACL has a header that indicates whether auditing is triggered by success, failure, or both; a SID that specifies a particular user or security group to monitor; and an access mask that lists the operations to audit.

The SACL also MAY contain[<68>](#Appendix_A_68" \o "Product behavior note 68) a label ACE that defines the integrity level of the object.

The only valid ACE types for a SACL are the auditing types (SYSTEM\_AUDIT\_ACE\_TYPE, SYSTEM\_AUDIT\_OBJECT\_ACE\_TYPE, SYSTEM\_AUDIT\_CALLBACK\_ACE\_TYPE, and SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE\_TYPE), the label type (SYSTEM\_MANDATORY\_LABEL\_ACE\_TYPE), the system resource attribute type (SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE\_TYPE), and the scoped policy type (SYSTEM\_SCOPED\_POLICY\_ID\_ACE\_TYPE), as specified in section 2.4.4.1.

The SACL MUST NOT contain ACEs that belong in the DACL, and the DACL MUST NOT contain ACE types that belong in the SACL. Doing so results in unspecified behavior.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| AclRevision | | | | | | | | Sbz1 | | | | | | | | AclSize | | | | | | | | | | | | | | | |
| AceCount | | | | | | | | | | | | | | | | Sbz2 | | | | | | | | | | | | | | | |

**AclRevision (1 byte):** An unsigned 8-bit value that specifies the revision of the ACL. The only two legitimate forms of ACLs supported for on-the-wire management or manipulation are type 2 and type 4. No other form is valid for manipulation on the wire. Therefore this field MUST be set to one of the following values.

| Value | Meaning |
| --- | --- |
| ACL\_REVISION  0x02 | When set to 0x02, only **AceTypes** 0x00, 0x01, 0x02, 0x03, 0x11, 0x12, and 0x13 can be present in the ACL. An **AceType** of 0x11 is used for SACLs but not for DACLs. For more information about ACE types, see section 2.4.4.1. |
| ACL\_REVISION\_DS  0x04 | When set to 0x04, **AceTypes** 0x05, 0x06, 0x07, 0x08, and 0x11 are allowed. ACLs of revision 0x04 are applicable only to directory service objects. An **AceType** of 0x11 is used for SACLs but not for DACLs. |

**Sbz1 (1 byte):** An unsigned 8-bit value. This field is reserved and MUST be set to zero.

**AclSize (2 bytes):** An unsigned 16-bit integer that specifies the size, in bytes, of the complete ACL, including all ACEs.

**AceCount (2 bytes):** An unsigned 16-bit integer that specifies the count of the number of ACE records in the ACL.

**Sbz2 (2 bytes):** An unsigned 16-bit integer. This field is reserved and MUST be set to zero.

#### ACL--RPC Representation

The RPC representation of the [ACL](#Section_20233ed8a6c64097aafadd545ed24428) data type specifies the elements needed to access a complete access control list, including both the ACL header structure and the array of [ACEs](#Section_d06e5a81176e46c69cf79137aad4455e). The individual members are as specified in section 2.4.5.

The ACL structure MUST be aligned on a 32-bit boundary.

In the absence of implementation-specific functions to access the individual ACEs, access to each ACE MUST be computed by using the **AclSize** and **AceCount** members to parse the memory following the ACL to identify each [ACE\_HEADER](#Section_628ebb1dc5094ea0a10f77ef97ca4586), which in turn contains the information needed to obtain the specific ACEs.

1. typedef struct \_ACL {
2. unsigned char AclRevision;
3. unsigned char Sbz1;
4. unsigned short AclSize;
5. unsigned short AceCount;
6. unsigned short Sbz2;
7. } ACL,
8. \*PACL;

### SECURITY\_DESCRIPTOR

The SECURITY\_DESCRIPTOR structure defines the security attributes of an object. These attributes specify who owns the object; who can access the object and what they can do with it; what level of audit logging can be applied to the object; and what kind of restrictions apply to the use of the security descriptor.

Security descriptors appear in one of two forms, absolute or self-relative.

A security descriptor is said to be in absolute format if it stores all of its security information via pointer fields, as specified in the RPC representation in section [2.4.6.1](#Section_f1e181673ddf48ada3d4b7e832f96b95).

A security descriptor is said to be in self-relative format if it stores all of its security information in a contiguous block of memory and expresses all of its pointer fields as offsets from its beginning. The order of appearance of pointer target fields is not required to be in any particular order; the location of the OwnerSid, GroupSid, Sacl, and/or Dacl is only based on OffsetOwner, OffsetGroup, OffsetSacl, and/or OffsetDacl pointers found in the fixed portion of the relative security descriptor.[<69>](#Appendix_A_69" \o "Product behavior note 69)

The self-relative form of the security descriptor is required if one wants to transmit the SECURITY\_DESCRIPTOR structure as an opaque data structure for transmission in communication protocols over a wire, or for storage on secondary media; the absolute form cannot be transmitted because it contains pointers to objects that are generally not accessible to the recipient.

When a self-relative security descriptor is transmitted over a wire, it is sent in [**little-endian**](#gt_079478cb-f4c5-4ce5-b72b-2144da5d2ce7) format and requires no padding.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Revision | | | | | | | | Sbz1 | | | | | | | | Control | | | | | | | | | | | | | | | |
| OffsetOwner | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OffsetGroup | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OffsetSacl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OffsetDacl | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OwnerSid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| GroupSid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sacl (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Dacl (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Revision (1 byte):** An unsigned 8-bit value that specifies the revision of the SECURITY\_DESCRIPTOR structure. This field MUST be set to one.

**Sbz1 (1 byte):** An unsigned 8-bit value with no meaning unless the **Control** RM bit is set to 0x1. If the RM bit is set to 0x1, **Sbz1** is interpreted as the [**resource manager**](#gt_a7d0361f-8608-454d-9a52-67d4d181ae09) control bits that contain specific information[<70>](#Appendix_A_70" \o "Product behavior note 70) for the specific resource manager that is accessing the structure. The permissible values and meanings of these bits are determined by the implementation of the resource manager.

**Control (2 bytes):** An unsigned 16-bit field that specifies control access bit flags. The Self Relative (SR) bit MUST be set when the security descriptor is in self-relative format.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1 0 | 1 | 2 | 3 | 4 | 5 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S  R | R  M | P  S | P  D | S  I | D  I | S  C | D  C | S  S | D  T | S  D | S  P | D  D | D  P | G  D | O  D |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| SR  Self-Relative | Set when the security descriptor is in self-relative format. Cleared when the security descriptor is in absolute format. |
| RM  RM Control Valid | Set to 0x1 when the **Sbz1** field is to be interpreted as resource manager control bits. |
| PS  SACL Protected | Set when the SACL will be protected from inherit operations. |
| PD  DACL Protected | Set when the DACL will be protected from inherit operations. |
| SI  SACL Auto-Inherited | Set when the SACL was created through inheritance. |
| DI  DACL Auto-Inherited | Set when the DACL was created through inheritance. |
| SC  SACL Computed Inheritance Required | Set when the SACL is to be computed through inheritance. When both SC and SI are set, the resulting security descriptor sets SI; the SC setting is not preserved. |
| DC  DACL Computed Inheritance Required | Set when the DACL is to be computed through inheritance. When both DC and DI are set, the resulting security descriptor sets DI; the DC setting is not preserved. |
| SS  Server Security | Set when the caller wants the system to create a Server ACL based on the input ACL, regardless of its source (explicit or defaulting). |
| DT  DACL Trusted | Set when the ACL that is pointed to by the **DACL** field was provided by a trusted source and does not require any editing of compound ACEs. |
| SD  SACL Defaulted | Set when the SACL was established by default means. |
| SP  SACL Present | Set when the SACL is present on the object. |
| DD  DACL Defaulted | Set when the DACL was established by default means. |
| DP  DACL Present | Set when the DACL is present on the object. |
| GD  Group Defaulted | Set when the group was established by default means. |
| OD  Owner Defaulted | Set when the owner was established by default means. |

**OffsetOwner (4 bytes):** An unsigned 32-bit integer that specifies the offset to the [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25). This SID specifies the owner of the object to which the security descriptor is associated. This must be a valid offset if the OD flag is not set. If this field is set to zero, the **OwnerSid** field MUST not be present.

**OffsetGroup (4 bytes):** An unsigned 32-bit integer that specifies the offset to the SID. This SID specifies the group of the object to which the security descriptor is associated. This must be a valid offset if the GD flag is not set. If this field is set to zero, the **GroupSid** field MUST not be present.

**OffsetSacl (4 bytes):** An unsigned 32-bit integer that specifies the offset to the [ACL](#Section_20233ed8a6c64097aafadd545ed24428) that contains system ACEs. Typically, the system ACL contains auditing ACEs (such as [SYSTEM\_AUDIT\_ACE](#Section_9431fd0f5b9a47f0b3f03015e2d0d4f9), [SYSTEM\_AUDIT\_CALLBACK\_ACE](#Section_bd6b6fd84bef427e9a43b9b46457e934), or [SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE](#Section_949b02e7f55d4c26969f52a009597469)), and at most one Label ACE (as specified in section [2.4.4.13](#Section_25fa65656cb046aba30a016b32c4939a)). This must be a valid offset if the SP flag is set; if the SP flag is not set, this field MUST be set to zero. If this field is set to zero, the **Sacl** field MUST not be present.

**OffsetDacl (4 bytes):** An unsigned 32-bit integer that specifies the offset to the ACL that contains ACEs that control access. Typically, the DACL contains ACEs that grant or deny access to principals or groups. This must be a valid offset if the DP flag is set; if the DP flag is not set, this field MUST be set to zero. If this field is set to zero, the **Dacl** field MUST not be present.

**OwnerSid (variable):** The SID of the owner of the object. The length of the SID MUST be a multiple of 4. This field MUST be present if the **OffsetOwner** field is not zero.

**GroupSid (variable):** The SID of the group of the object. The length of the SID MUST be a multiple of 4. This field MUST be present if the **GroupOwner** field is not zero.[<71>](#Appendix_A_71" \o "Product behavior note 71)

**Sacl (variable):** The [**SACL**](#gt_c189801e-3752-4715-88f4-17804dad5782) of the object. The length of the SID MUST be a multiple of 4. This field MUST be present if the SP flag is set.

**Dacl (variable):** The [**DACL**](#gt_d727f612-7a45-48e4-9d87-71735d62b321) of the object. The length of the SID MUST be a multiple of 4. This field MUST be present if the DP flag is set.

#### SECURITY\_DESCRIPTOR--RPC Representation

The RPC representation of the SECURITY\_DESCRIPTOR structure defines the in-memory representation of the [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) message. The individual member semantics for the **Revision**, **Sbz1**, **Control**, **Owner**, **Group**, **Sacl** and **Dacl** members are as specified in section 2.4.6, with the exceptions that Owner corresponds to OwnerSid, and Group corresponds to GroupSid, respectively.

1. typedef struct \_SECURITY\_DESCRIPTOR {
2. UCHAR Revision;
3. UCHAR Sbz1;
4. USHORT Control;
5. PSID Owner;
6. PSID Group;
7. PACL Sacl;
8. PACL Dacl;
9. } SECURITY\_DESCRIPTOR,
10. \*PSECURITY\_DESCRIPTOR;

**Revision:**  As specified in section 2.4.6.

**Sbz1:**  As specified in section 2.4.6.

**Control:**  As specified in section 2.4.6.

**Owner:**  Pointer to the Owner SID (OwnerSid), as specified in section 2.4.6.

**Group:**  Pointer to the Group SID (GroupSid), as specified in section 2.4.6.

**Sacl:**  Pointer to the Sacl, as specified in section 2.4.6.

**Dacl:**  Pointer to the Dacl, as specified in section 2.4.6.

### SECURITY\_INFORMATION

The SECURITY\_INFORMATION data type identifies the object-related security information being set or queried. This security information includes:

* The owner of an object.
* The primary group of an object.
* The discretionary access control list (DACL) of an object.
* The system access control list (SACL) of an object.

An unsigned 32-bit integer specifies portions of a [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) by means of bit flags. Individual bit values (combinable with the bitwise OR operation) are as shown in the following table.

| Value | Meaning |
| --- | --- |
| OWNER\_SECURITY\_INFORMATION  0x00000001 | The owner identifier of the object is being referenced. |
| GROUP\_SECURITY\_INFORMATION  0x00000002 | The primary group identifier of the object is being referenced. |
| DACL\_SECURITY\_INFORMATION  0x00000004 | The DACL of the object is being referenced. |
| SACL\_SECURITY\_INFORMATION  0x00000008 | The SACL of the object is being referenced. |
| LABEL\_SECURITY\_INFORMATION  0x00000010 | The mandatory integrity label is being referenced. |
| UNPROTECTED\_SACL\_SECURITY\_INFORMATION  0x10000000 | The SACL inherits access control entries (ACEs) from the parent object. |
| UNPROTECTED\_DACL\_SECURITY\_INFORMATION  0x20000000 | The DACL inherits ACEs from the parent object. |
| PROTECTED\_SACL\_SECURITY\_INFORMATION  0x40000000 | The SACL cannot inherit ACEs. |
| PROTECTED\_DACL\_SECURITY\_INFORMATION  0x80000000 | The DACL cannot inherit ACEs. |
| ATTRIBUTE\_SECURITY\_INFORMATION  0x00000020 | A [SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE](#Section_352944c74fb6498880360a25dcedc730) (section 2.4.4.15) is being referenced. |
| SCOPE\_SECURITY\_INFORMATION  0x00000040 | A [SYSTEM\_SCOPED\_POLICY\_ID\_ACE](#Section_aa0c0f624b4c44f09718c266a6accd9f) (section 2.4.4.16) is being referenced. |
| BACKUP\_SECURITY\_INFORMATION  0x00010000 | The security descriptor is being accessed for use in a backup operation. |

This type is declared as follows:

1. typedef DWORD SECURITY\_INFORMATION, \*PSECURITY\_INFORMATION;

### TOKEN\_MANDATORY\_POLICY

The TOKEN\_MANDATORY\_POLICY structure specifies the mandatory integrity policy for a [token](#Section_efc83c3252754dffa3e2973c9624711b).

1. typedef struct \_TOKEN\_MANDATORY\_POLICY {
2. DWORD Policy;
3. } TOKEN\_MANDATORY\_POLICY,
4. \*PTOKEN\_MANDATORY\_POLICY;

**Policy:**  The **Policy** member contains a value denoting the mandatory integrity policy of the token; these values are mutually exclusive.

| Value | Meaning |
| --- | --- |
| TOKEN\_MANDATORY\_POLICY\_OFF  0x00000000 | No mandatory integrity policy is enforced for the token. |
| TOKEN\_MANDATORY\_POLICY\_NO\_WRITE\_UP  0x00000001 | A process associated with the token cannot write to objects that have a greater mandatory integrity level. |
| TOKEN\_MANDATORY\_POLICY\_NEW\_PROCESS\_MIN  0x00000002 | A process created with the token has an integrity level that is the lesser of the parent-process integrity level and the executable-file integrity level. |

### MANDATORY\_INFORMATION

The MANDATORY\_INFORMATION structure defines mandatory security information for a securable object.

1. typedef struct \_MANDATORY\_INFORMATION {
2. ACCESS\_MASK AllowedAccess;
3. BOOLEAN WriteAllowed;
4. BOOLEAN ReadAllowed;
5. BOOLEAN ExecuteAllowed;
6. TOKEN\_MANDATORY\_POLICY MandatoryPolicy;
7. } MANDATORY\_INFORMATION,
8. \*PMANDATORY\_INFORMATION;

**AllowedAccess:**  The **AllowedAccess** member specifies the access mask that is used to encode the user rights to an object.

**WriteAllowed:**  Specifies write properties for the object.

**ReadAllowed:**  Specifies read properties for the object.

**ExecuteAllowed:**  Specifies execution properties for the object.

**MandatoryPolicy:**  Specifies the integrity policy for the object.

### CLAIM\_SECURITY\_ATTRIBUTE

The CLAIM\_SECURITY\_ATTRIBUTE type specifies a security attribute (also called a security claim) in various formats.

#### CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1

The CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure defines a resource attribute that is defined in contiguous memory for persistence within a serialized Security Descriptor.

1. typedef struct \_CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 {
2. DWORD Name;
3. WORD ValueType;
4. WORD Reserved;
5. DWORD Flags;
6. DWORD ValueCount;
7. union {
8. PLONG64 pInt64[];
9. PDWORD64 pUint64[];
10. PWSTR ppString[];
11. PCLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE pOctetString[];
12. } Values;
13. } CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1,
14. \*PCLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1;

**Name:**  A [DWORD](#Section_262627d83418462792184ffe110850b2) value indicating an offset from the beginning of the CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure to a string of Unicode characters containing the name of the claim security attribute. The string MUST be at least 4 bytes in length.

**ValueType:**  A union tag value indicating the type of information referred to by the Values member. The **Values** member MUST be an array of offsets from the beginning of the CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure to the specified **ValueType**. **ValueType** MUST be one of the following values:

| Value | Meaning |
| --- | --- |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_INT64  0x0001 | **Values** member refers to an array of offsets to [LONG64](#Section_7dc8dc9c9d54417a933e173933f0c329) value(s). |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_UINT64  0x0002 | **Values** member refers to an array of offsets to [ULONG64](#Section_2dc4c49295db4fa6ae2b8546b13c9141) value(s). |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_STRING  0x0003 | **Values** member refers to an array of offsets to [**Unicode character**](#gt_fd33af2e-e1ce-4f8e-a706-f9fb8123f9b0) string value(s). |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_SID  0x0005 | The **Values** member refers to an array of offsets to [CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE](#Section_9020a075c1af4b03930bba785743bcab) value(s) where the OctetString value is a [SID](#Section_c92a27b1c7724fa7a43215df5f1b66a1) string. |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_BOOLEAN  0x0006 | The **Values** member refers to an array of offsets to ULONG64 values where each element indicates a Boolean value. The value 1 indicates TRUE, and the value 0 indicates FALSE. |
| CLAIM\_SECURITY\_ATTRIBUTE\_TYPE\_OCTET\_STRING  0x0010 | **Values** member contains an array of CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE value(s) as specified in section 2.4.10.2. |

**Reserved:**  Reserved. This member MUST be set to zero when sent and MUST be ignored when received.

**Flags:**  The upper two bytes of this DWORD are available for application-specific data. The two lowest-order bits in the lower of these two bytes are reserved. These two bytes MAY[<72>](#Appendix_A_72" \o "Product behavior note 72) contain only one of the following values in those two bits:

| Value | Meaning |
| --- | --- |
| FCI\_CLAIM\_SECURITY\_ATTRIBUTE\_MANUAL  0x0001 | The CLAIM\_SECURITY\_ATTRIBUTE has been manually assigned. |
| FCI\_CLAIM\_SECURITY\_ATTRIBUTE\_POLICY\_DERIVED  0x0002 | The CLAIM\_SECURITY\_ATTRIBUTE has been determined by a central policy. |

The lower two bytes of this DWORD MUST be zero or a bitwise combination of one or more of the following values:[<73>](#Appendix_A_73" \o "Product behavior note 73)

| Value | Meaning |
| --- | --- |
| CLAIM\_SECURITY\_ATTRIBUTE\_NON\_INHERITABLE  0x0001 | This claim security attribute is not inherited across processes.[<74>](#Appendix_A_74" \o "Product behavior note 74) |
| CLAIM\_SECURITY\_ATTRIBUTE\_VALUE\_CASE\_SENSITIVE  0x0002 | The value of the claim security attribute is case sensitive. This flag is valid for values that contain string types. |
| CLAIM\_SECURITY\_ATTRIBUTE\_USE\_FOR\_DENY\_ONLY  0x0004 | Reserved for future use. |
| CLAIM\_SECURITY\_ATTRIBUTE\_DISABLED\_BY\_DEFAULT  0x0008 | The claim security attribute is disabled by default. |
| CLAIM\_SECURITY\_ATTRIBUTE\_DISABLED  0x0010 | Reserved for future use. |
| CLAIM\_SECURITY\_ATTRIBUTE\_MANDATORY  0x0020 | The claim security attribute is mandatory. |

**ValueCount:**  The number of values contained in the **Values** member.

**Values:**  An array of offsets from the beginning of the CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure. Each offset indicates the location of a claim security attribute value of type specified in the **ValueType** member.

#### CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE

The CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE structure specifies an octet string.[<75>](#Appendix_A_75" \o "Product behavior note 75)

1. typedef struct \_CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE {
2. DWORD Length;
3. BYTE OctetString[];
4. } CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE,
5. \*PCLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE;

**Length:**  The length, in bytes, of the value contained in the **OctetString** field.

**OctetString:**  An array of bytes containing the octet string value. The length of the value is specified by the **Length** field.

## Additional Information for Security Types

### Security Descriptor Description Language

The [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) structure is a compact binary representation of the security associated with an object in a directory or on a file system, or in other stores. It is not, however, convenient for use in tools that operate primarily on text strings. Therefore, a text-based form of the security descriptor is available for situations when a security descriptor must be carried by a text method. This format is the Security Descriptor Description Language (SDDL).[<76>](#Appendix_A_76" \o "Product behavior note 76)

For more information on SDDL for Device Objects, see [[MSDN-SDDLforDevObj]](https://go.microsoft.com/fwlink/?LinkId=114214).

#### Syntax

An SDDL string is a single sequence of characters. The format can be [**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583) or [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8); the actual protocol MUST specify the character set that is used. Regardless of the character set used, the characters that can be used are alphanumeric and punctuation.

The format for an SDDL string is described by the following ABNF (as specified in [[RFC5234]](https://go.microsoft.com/fwlink/?LinkId=123096)) grammar, where the elements are as shown here.[<77>](#Appendix_A_77" \o "Product behavior note 77)

1. sddl = [owner-string] [group-string] [dacl-string] [sacl-string]
2. owner-string = "O:" sid-string
3. group-string = "G:" sid-string
4. dacl-string = "D:" [acl-flag-string] [aces]
5. sacl-string = "S:" [acl-flag-string] [aces]
6. sid-string = sid-token / sid-value
7. sid-value = SID;defined in section 2.4.2.1
8. sid-token = "DA"/ "DG" / "DU" / "ED" / "DD" / "DC" / "BA" / "BG" / "BU" /
9. "LA" / "LG" / "AO" / "BO" / "PO" / "SO" / "AU" / "PS" / "CO" / "CG" / "SY" /
10. "PU" / "WD" / "RE" / "IU" / "NU" / "SU" / "RC" / "WR" / "AN" / "SA" / "CA" /
11. "RS" / "EA" / "PA" / "RU" / "LS" / "NS" / "RD" / "NO" / "MU" / "LU" / "IS" /
12. "CY" / "OW" / "ER" / "RO" / "CD" / "AC" / "RA" / "ES" / "MS" / "UD" / "HA" /
13. "CN" / "AA" / "RM" / "LW" / "ME" /"MP" / "HI" / "SI"
14. acl-flag-string = \*acl-flag
15. acl-flag = "P" / "AR" / "AI"
16. aces = \*(ace / conditional-ace / resource-attribute-ace)
17. ace = "(" ace-type ";" [ace-flag-string] ";" ace-rights ";"
18. [object-guid] ";" [inherit-object-guid] ";" sid-string ")"
19. ace-type = "A" / "D" / "OA" / "OD" / "AU" / "OU" / "ML" / "SP"
20. conditional-ace = "(" conditional-ace-type ";" [ace-flag-string] ";" ace-rights
21. ";" [object-guid] ";" [inherit-object-guid] ";" sid-string ";" "(" cond-expr ")" ")"
22. conditional-ace-type = "XA" / "XD" / "ZA" / "XU"
23. central-policy-ace = "(" "SP" ";" [ace-flag-string] ";;;;" capid-value-sid")"
24. capid-value-sid = "S-1-17-" 1\*SubAuthority
25. ; SubAuthority defined in section 2.4.2.1
26. resource-attribute-ace = "(" "RA" ";" [ace-flag-string] ";;;;" ( "WD" /
27. "S-1-1-0" ) ";(" attribute-data "))"
28. attribute-data = DQUOTE 1\*attr-char2 DQUOTE "," ( TI-attr / TU-attr / TS-attr /
29. TD-attr / TX-attr / TB-attr )
30. TI-attr = "TI" "," attr-flags \*("," int-64)
31. TU-attr = "TU" "," attr-flags \*("," uint-64)
32. TS-attr = "TS" "," attr-flags \*("," char-string)
33. TD-attr = "TD" "," attr-flags \*("," sid-string)
34. TX-attr = "TX" "," attr-flags \*("," octet-string)
35. TB-attr = "TB" "," attr-flags \*("," ( "0" / "1" ) )
36. attr-flags = "0x" ([\*4HEXDIG "00"] sys-attr-flags / \*"0" sys-attr-flags /
37. \*"0" HEXDIG)
38. sys-attr-flags = ( "0"/ "1" / "2" / "3" ) HEXDIG
39. ace-flag-string = ace-flag ace-flag-string / ""
40. ace-flag = "CI" / "OI" / "NP" / "IO" / "ID" / "SA" / "FA"
41. ace-rights = (\*text-rights-string) / ("0x" 1\*8HEXDIG) / ("0" 1\*%x30-37) /
42. (1\*DIGIT )
43. ; numeric values must fit within 64 bits
44. text-rights-string = generic-rights-string / standard-rights-string /
45. object-specific-rights-string
46. generic-rights-string = generic-right / generic-rights-string / ""
47. generic-right = "GA" / "GW" / "GR" / "GX"
48. standard-rights-string = standard-right / standard-rights-string / ""
49. standard-right = "WO" / "WD" / "RC" / "SD"
50. object-specific-rights-string = object-specific-right / object-specific-
51. rights-string / ""
52. object-specific-right = <any object-specific right, for objects like files,
53. registry keys, directory objects, and others>
54. guid = "" / 8HEXDIG "-" 4HEXDIG "-" 4HEXDIG "-" 4HEXDIG "-" 12HEXDIG
55. ; The second option is the GUID of the object in the form
56. ; "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" Where each "X" is a Hex digit
57. object-guid = guid
58. inherit-object-guid = guid
59. wspace = 1\*(%x09-0D / %x20)
60. term = [wspace] (memberof-op / exists-op / rel-op / contains-op / anyof-op / attr-name
61. / rel-op2) [wspace]
62. cond-expr = term / term [wspace] ("||" / "&&" ) [wspace] cond-expr / (["!"] [wspace]
63. "(" cond-expr ")")
64. memberof-op = ( "Member\_of" / "Not\_Member\_of" / "Member\_of\_Any" /
65. "Not\_Member\_of\_Any" / "Device\_Member\_of" / "Device\_Member\_of\_Any" /
66. "Not\_Device\_Member\_of" / "Not\_Device\_Member\_of\_Any" ) wspace sid-array
67. exists-op = ( "Exists" / "Not\_exists") wspace attr-name
68. rel-op = attr-name [wspace] ("<" / "<=" / ">" / ">=") [wspace] (attr-name2 / value)
69. ; only scalars
70. rel-op2 = attr-name [wspace] ("==" / "!=") [wspace] ( attr-name2 / value-array )
71. ; scalar or list
72. contains-op = attr-name wspace ("Contains" / "Not\_Contains") wspace (attr-name2 / value-array)
73. anyof-op = attr-name wspace ("Any\_of" / "Not\_Any\_of") wspace (attr-name2 / value-array)
74. attr-name1 = attr-char1 \*(attr-char1 / "@")
75. ; old simple name
76. attr-char1 = 1\*(ALPHA / DIGIT / ":" / "." / "/" / "\_")
77. attr-name2 = ("@user." / "@device." / "@resource.") 1\*attr-char2
78. ; new prefixed name form
79. attr-char2 = attr-char1 / lit-char
80. attr-name = attr-name1 / attr-name2
81. ; either name form
82. sid-array = literal-SID [wspace] / "{" [wspace] literal-SID [wspace] \*( "," [wspace] literal-SID [wspace]) "}"
83. literal-SID = "SID(" sid-string ")"
84. value-array = value [wspace] / "{" [wspace] value [wspace] \*("," [wspace] value [wspace]) "}"
85. value = int-64 / char-string / octet-string
86. int-64 = ["+" / "-"] ("0x" 1\*HEXDIG) / ("0" 1\*%x30-37) / 1\*DIGIT
87. ; values must fit within 64 bits in two's complement form
88. uint-64 = ("0x" 1\*HEXDIG) / ("0" 1\*%x30-37) / 1\*DIGIT
89. ; values must fit within 64 bits
90. char-string = DQUOTE \*(CHAR) DQUOTE
91. octet-string = "#" \*(2HEXDIG)
92. lit-char = "#" / "$" / "'" / "\*" / "+" / "-" / "." / "/" / ":" / ";" / "?" /
93. "@" / "[" / "\" / "]" / "^" / "\_" / "`" / "{" / "}" / "~" / %x0080-FFFF /
94. ( "%" 4HEXDIG)
95. ; 4HEXDIG can have any value except 0000 (NULL)

**sid-token**: An abbreviated form of a well-known SID, per the following table.

| SDDL alias | Well-Known SID name |
| --- | --- |
| "DA" | DOMAIN\_ADMINS |
| "DG" | DOMAIN\_GUESTS |
| "DU" | DOMAIN\_USERS |
| "ED" | ENTERPRISE\_DOMAIN\_CONTROLLERS |
| "DD" | DOMAIN\_DOMAIN\_CONTROLLERS |
| "DC" | DOMAIN\_COMPUTERS |
| "BA" | BUILTIN\_ADMINISTRATORS |
| "BG" | BUILTIN\_GUESTS |
| "BU" | BUILTIN\_USERS |
| "LA" | ADMINISTRATOR[<78>](#Appendix_A_78" \o "Product behavior note 78) |
| "LG" | GUEST |
| "AO" | ACCOUNT\_OPERATORS |
| "BO" | BACKUP\_OPERATORS |
| "PO" | PRINTER\_OPERATORS |
| "SO" | SERVER\_OPERATORS |
| "AU" | AUTHENTICATED\_USERS |
| "PS" | PRINCIPAL\_SELF |
| "CO" | CREATOR\_OWNER |
| "CG" | CREATOR\_GROUP |
| "SY" | LOCAL\_SYSTEM |
| "PU" | POWER\_USERS |
| "WD" | EVERYONE |
| "RE" | REPLICATOR |
| "IU" | INTERACTIVE |
| "NU" | NETWORK |
| "SU" | SERVICE |
| "RC" | RESTRICTED\_CODE |
| "WR" | WRITE\_RESTRICTED\_CODE |
| "AN" | ANONYMOUS |
| "SA" | SCHEMA\_ADMINISTRATORS |
| "CA" | CERT\_PUBLISHERS |
| "RS" | RAS\_SERVERS |
| "EA" | ENTERPRISE\_ADMINS |
| "PA" | GROUP\_POLICY\_CREATOR\_OWNER |
| "RU" | ALIAS\_PREW2KCOMPACC |
| "LS" | LOCAL\_SERVICE |
| "NS" | NETWORK\_SERVICE |
| "RD" | REMOTE\_DESKTOP |
| "NO" | NETWORK\_CONFIGURATION\_OPS |
| "MU" | PERFMON\_USERS |
| "LU" | PERFLOG\_USERS |
| "IS" | IIS\_USERS |
| "CY" | CRYPTO\_OPERATORS |
| "OW" | OWNER\_RIGHTS |
| "ER" | EVENT\_LOG\_READERS |
| "RO" | ENTERPRISE\_RO\_DCS |
| "CD" | CERTSVC\_DCOM\_ACCESS |
| "AC" | ALL\_APP\_PACKAGES |
| "RA" | RDS\_REMOTE\_ACCESS\_SERVERS |
| "ES" | RDS\_ENDPOINT\_SERVERS |
| "MS" | RDS\_MANAGEMENT\_SERVERS |
| "UD" | USER\_MODE\_DRIVERS |
| "HA" | HYPER\_V\_ADMINS |
| "CN" | CLONEABLE\_CONTROLLERS |
| "AA" | ACCESS\_CONTROL\_ASSISTANCE\_OPS |
| "RM" | REMOTE\_MANAGEMENT\_USERS |
| "LW" | ML\_LOW |
| "ME" | ML\_MEDIUM |
| "MP" | ML MEDIUM PLUS |
| "HI" | ML\_HIGH |
| "SI" | ML\_SYSTEM |

**acl-flag**: Flags for the [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) structure, context dependent on whether a SACL or DACL is being processed. These flags are derived from the SECURITY\_DESCRIPTOR **Control** flags specified in section 2.4.6. "P" indicates Protected PS or PD flags from that section, "AR" corresponds to SC or DC, and "AI" indicates SI or DI.

**ace-type**: String that indicates the type of ACE that is being presented.

| String | ACE type |
| --- | --- |
| "A" | Access Allowed |
| "D" | Access Denied |
| "AU" | Audit |
| "OA" | Object Access Allowed |
| "OD" | Object Access Denied |
| "OU" | Object Audit |
| "ML" | Mandatory Label |
| "SP" | Central Policy ID |

**conditional-ace-type**: String that indicates the type of SDDL-supported conditional ACE that is being presented.[<79>](#Appendix_A_79" \o "Product behavior note 79)

| String | ACE type | Numeric value |
| --- | --- | --- |
| "XA" | Access Allowed Callback | 0x9 |
| "XD" | Access Denied Callback | 0xA |
| "XU" | Access Allowed Object Callback | 0xB |
| "ZA" | Audit Callback | 0xD |

**central-policy-ace**: An ACE type that identifies a central policy to be applied to the resource. Also called a [SYSTEM\_SCOPED\_POLICY\_ID ACE](#Section_aa0c0f624b4c44f09718c266a6accd9f) (see section 2.4.4.16).[<80>](#Appendix_A_80" \o "Product behavior note 80)

**capid-value-sid**: A SID with an Authority value of 17 that refers to a CentralAccessPolicy within a CentralAccessPolicysList ([[MS-GPCAP]](%5bMS-GPCAP%5d.pdf#Section_5189d5c912c2491cbf16f7008c46c6fb) section 3.2.1.1).[<81>](#Appendix_A_81" \o "Product behavior note 81)

**resource-attribute-ace**: An ACE type that defines a resource attribute (sometimes referred to as a resource property or resource claim.) See section [2.4.4.15](#Section_352944c74fb6498880360a25dcedc730).[<82>](#Appendix_A_82" \o "Product behavior note 82)

**attribute-data**: A string specifying the name of a resource attribute and data defining the type and value of the attribute. A resource attribute type can be identified with one of the following strings:[<83>](#Appendix_A_83" \o "Product behavior note 83)

| String | Resource Attribute Type |
| --- | --- |
| "TI" | 64-bit Integer |
| "TU" | Unsigned 64-bit integer |
| "TS" | String of Unicode characters |
| "TD" | A SID in string form |
| "TX" | A string of single byte (octet) values |
| "TB" | A string containing a Boolean value represented by a "1" (True) or a "0" (False.) |

**attr-flags**: A 32-bit number containing flag values within a resource attribute. The bits 16-31 can contain custom values. Bits 0 through 15 are specified by sys-attr-flags.

**sys-attr-flags**: A two-byte integer that MAY be zero or any combination of the hexadecimal flag values of the [CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#Section_21f2b5f0737645bbbc31eaa60841dbe9) structure (section 2.4.10.1)

**ace-flag-string**: A set of ACE flags that define the behavior of the ACE. The strings correlate exactly to the flags as specified in section [2.4.4.1](#Section_628ebb1dc5094ea0a10f77ef97ca4586).

**generic-rights-string**: A set of generic user rights used to perform generic mappings to object-specific rights.

| String | Access right | Hex value |
| --- | --- | --- |
| "GR" | Generic Read | 0x80000000 |
| "GW" | Generic Write | 0x40000000 |
| "GX" | Generic Execute | 0x20000000 |
| "GA" | Generic All | 0x10000000 |

**standard-rights-string**: A set of SDDL-supported standard user rights.

| String | Access right | Hex value |
| --- | --- | --- |
| "WO" | Write Owner | 0x00080000 |
| "WD" | Write DAC | 0x00040000 |
| "RC" | Read Control | 0x00020000 |
| "SD" | Delete | 0x00010000 |

**object-specific-rights-string**: A set of object-specific rights; some common ones are shown, but the it is recommended that the reader consult a specific protocol for applicable values, if any, in that protocol.

| String | Object type | Access right | Hex value |
| --- | --- | --- | --- |
| "FA" | File | File All Access | 0x001F01FF |
| "FX" | File | File Execute | 0x001200A0 |
| "FW" | File | File Write | 0x00120116 |
| "FR" | File | File Read | 0x00120089 |
| "KA" | Registry Key | Key All Access | 0x000F003F |
| "KR" | Registry Key | Key Read | 0x00020019 |
| "KX" | Registry Key | Key Execute | 0x00020019 |
| "KW" | Registry Key | Key Write | 0x00020006 |
| "CR" | Directory Object | Control Access | 0x00000100 |
| "LO" | Directory Object | List Object | 0x00000080 |
| "DT" | Directory Object | Delete Tree | 0x00000040 |
| "WP" | Directory Object | Write Property | 0x00000020 |
| "RP" | Directory Object | Read Property | 0x00000010 |
| "SW" | Directory Object | Self Write | 0x00000008 |
| "LC" | Directory Object | List Children | 0x00000004 |
| "DC" | Directory Object | Delete Child | 0x00000002 |
| "CC" | Directory Object | Create Child | 0x00000001 |

**term**: A string specifying a stand-alone logical expression, which is the simplest form of conditional expression, or a part of a more complex conditional expression.

**cond-expr**: A conditional expression in textual form. Conditional expressions are specified in section [2.4.4.17](#Section_10dc22eb788d4343b5560b6969fe58ca).

**memberof-op**: A string identifying a Member\_of type of operator as described in section [2.4.4.17.6](#Section_1711ff81cf134870919db91dca7e50de). [<84>](#Appendix_A_84" \o "Product behavior note 84)

**exists-op**: A string identifying an exists type operator as described in section [2.4.4.17.7](#Section_6e92a8b360d84cc08441dd6ba6e59e63).

**rel-op**: A string specifying a binary relational operation containing an attribute name or reference, one of the following relational operators, "==" , "!=" , "<" , "<=" , ">" , ">=" (without quotes) identifying a relational operator as described in section 2.4.4.17.6, and an attribute name or literal value.

**rel-op2**: A string specifying a binary operator for certain operators that support set comparisons. The string contains an attribute name, a string specifying the operator, "==" or "!=", and a string specifying an array of values (**value-array**).[<85>](#Appendix_A_85" \o "Product behavior note 85)

**contains-op**: A string specifying a relational operator term using a Contains or Not\_Contains operator.[<86>](#Appendix_A_86" \o "Product behavior note 86)

**anyof-op**: A string specifying a relational operator term using an Any\_of or Not\_Any\_of operator.[<87>](#Appendix_A_87" \o "Product behavior note 87)

**sid-array**: A string representation of an array of string SIDs.

**literal-SID**: A string specifying a literal SID. A literal-SID MUST be prefixed by the string "SID" followed by a sid-value enclosed in parentheses.

**attr-name1**: A string representing a valid attribute name in simple form.[<88>](#Appendix_A_88" \o "Product behavior note 88) An attribute name in simple form MUST not begin with the "@" character and MUST be comprised only of characters defined by attr-char1. An example of an attribute in simple form is "Title" (without quotes.) See section [2.5.1.2.1](#Section_25b69603880a47b8a48935c8e2fb7376).

**attr-name2**: A string representing a valid attribute name in @Prefixed form. An attribute name is in @Prefixed form when it is prefixed with the string "@User.", "@Device.", or "@Resource." and is comprised only of characters defined by attr-char2. An example of an attribute in @Prefixed form is "@User.Title" (without quotes.) See section [2.5.1.2.2](#Section_b30a934313904dc29e59b92fecfb4ac9).[<89>](#Appendix_A_89" \o "Product behavior note 89)

**attr-char1**: A character valid for use in an attribute name in simple form. Valid characters include any ALPHA or DIGIT (as specified in [RFC5234]) or any of the following: ":", ".", "/", "\_".

**attr-char2**: A character valid for use in an attribute name in @Prefixed form. Valid characters include all ASCII and UNICODE characters of the range 0x0-0xFFFF. Characters MAY be encoded either as literals or be encoded with a five-character sequence %XXXX, where XXXX are hexadecimal digits that represent the corresponding 16-bit Unicode value of the character with the following exceptions:

1. The following characters: "!", "&", "(", ")", ">", "<", "=", "|", "%", SP (space) and DQUOTE (as specified in [RFC5234]) MUST be encoded in the preceding five-character sequence.
2. The following characters MUST be encoded as literals: "#", "$", "'", "\*", "+", "-", ".", "/", ":", ";", "?", "@", "[", "\", "]", "^", "\_", "`", "{", "}", "~" and any characters in the ASCII ranges 0x41-0x5A (A-Z), 0x61-0x7A (a-z) and 0x30-0x39 (0-9.)

**value-array**: A string specifying an array of values. A value-array can be a single value or a set of one or more comma-delineated values where the entire set of values is enclosed between the "{" and "}" symbols.

#### Security Attribute Names

Attribute names are specially formatted strings used within conditional expressions to reference the attributes of a user, device, or resource. Attribute Names can be in simple or "@Prefixed" form.

##### Simple Attribute Name Form

An attribute name in simple form is limited to referencing an attribute in the **LocalClaims[]** array (section [2.5.2](#Section_efc83c3252754dffa3e2973c9624711b)) of the same name in simple form. An attribute name in simple form is case-insensitive and MAY contain any ALPHA or DIGIT (as specified in [RFC5234]) characters as well as the following characters: ":", ".", ", "\_". An attribute name in simple form MAY also contain the "@" character in any position other than the first character of the attribute name. See **attr-char1** in section [2.5.1.1](#Section_f4296d691c0f491f9587a960b292d070) for encoding requirements.

##### @Prefixed Attribute Name Form

The @Prefixed Attribute name form allows an attribute name to identify an attribute as being of type "User", "Device" or "Resource" and MUST follow the pattern:

1. @<attribute type>.<attribute name>

During policy evaluation, an attribute name in @Prefixed form references a user or device claim or resource attribute according to the following:

| "@"prefix Policy | evaluation reference |
| --- | --- |
| @User. | Claim of same name in UserClaims[] array of token/authorization context (section [2.5.2](#Section_efc83c3252754dffa3e2973c9624711b).) |
| @Device. | Claim of same name in DeviceClaims[] array of token/authorization context (section 2.5.2.) |
| @Resource. | Resource attribute of the same name encoded in the System Access Control List of the evaluated security descriptor as a [SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE](#Section_352944c74fb6498880360a25dcedc730) (section 2.4.4.15.) |

An attribute name in @Prefixed form is case-insensitive and valid characters include all [**ANSI**](#gt_100cd8a6-5cb1-4895-9de6-e4a3c224a583) and [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) characters of the range 0x0-0xFFFF. See **attr-char2** in section [2.5.1.1](#Section_f4296d691c0f491f9587a960b292d070) for encoding requirements.

#### Parentheses and Order of Precedence

SDDL expressions MUST be interpreted in the following order of precedence, with operations of equal precedence being evaluated from left to right. In addition, any term or conditional expression within a conditional expression can be enclosed in parentheses. Expressions within parentheses MUST be evaluated first.

1. Exists, Not\_Exists
2. Member\_of, Not\_Member\_of, Device\_Member\_of, Not\_Device\_Member\_of, Member\_of\_Any, Not\_Member\_of\_Any, Device\_Member\_of\_Any, Not\_Device\_Member\_of\_Any, Contains, Not\_Contains, Any\_of, Not\_Any\_of, ==, !=, <, <=, >, >=
3. !
4. &&
5. ||

#### SDDL String to Binary Security Descriptor Examples

The following SDDL string: "O:BAG:BAD:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)S:P(AU;FA;GR;;;WD)"

yields the following, which is an encoded output of the security descriptor in self-relative form ordered as [**little-endian**](#gt_079478cb-f4c5-4ce5-b72b-2144da5d2ce7).

1. 00000000 01 00 14 b0 90 00 00 00 a0 00 00 00 14 00 00 00 ................
2. 00000010 30 00 00 00 02 00 1c 00 01 00 00 00 02 80 14 00 0...............
3. 00000020 00 00 00 80 01 01 00 00 00 00 00 01 00 00 00 00 ................
4. 00000030 02 00 60 00 04 00 00 00 00 03 18 00 00 00 00 a0 ..'.............
5. 00000040 01 02 00 00 00 00 00 05 20 00 00 00 21 02 00 00 ........ ...!...
6. 00000050 00 03 18 00 00 00 00 10 01 02 00 00 00 00 00 05 ................
7. 00000060 20 00 00 00 20 02 00 00 00 03 14 00 00 00 00 10 ... ...........
8. 00000070 01 01 00 00 00 00 00 05 12 00 00 00 00 03 14 00 ................
9. 00000080 00 00 00 10 01 01 00 00 00 00 00 03 00 00 00 00 ................
10. 00000090 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 ........ ... ...
11. 000000a0 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 ........ ... ...

The [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) starts with the SD revision number (1 byte long) at address 0x00, followed by reserved bits and the SD control flags (2 bytes long). As mentioned previously, this is followed by owner, group, SACL, and DACL offsets.

1. 01 00 14 b0 90 00 00 00 a0 00 00 00 14 00 00 00

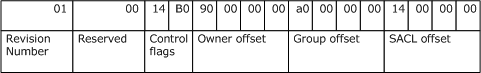


Figure 6: Security descriptor field offsets example

**Control Flags**

Control flags for the DACL are represented as a bitmask, and the resultant set of flags is computed by a logical OR of the flags. In this example, the control flag value is set to the following.

1. 1011000000010100

This control flag value maps to the meaning that is shown in the following table.

| BIT | Meaning |
| --- | --- |
| 0 | OD: Owner defaulted |
| 0 | GD: Group defaulted |
| 1 | DP: DACL present |
| 0 | DD: DACL defaulted |
| 1 | SP: SACL present |
| 0 | SD: SACL defaulted |
| 0 | SS: Server Security |
| 0 | DT: DACL Trusted |
| 0 | DR: DACL Inheritance Required |
| 0 | SR: Inheritance Required |
| 0 | DI: DACL auto-inherited |
| 0 | SI: SACL auto-inherited |
| 1 | PD: DACL-protected |
| 1 | PS: SACL-protected |
| 0 | RM: Control Valid |
| 1 | SR: Self-Relative |

**SACL**

The control flags are followed by the SACL, which in this example is "S:P(AU;FA;GR;;;WD)"

**DACL**

The SACL is followed by the SECURITY\_DESCRIPTOR DACL, which in this example is:

1. (A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)

**Note**  The string representation for the DACL (D:) and the DACL control flags are consumed not as part of the DACL structure in the SD, but instead as the security descriptor control flags. The same applies for SACL.

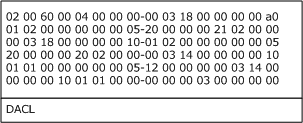


Figure 7: Security access control list data example

The ACL can be further dissected into the ACL header and the individual ACEs. For more information, see section [2.4.5](#Section_20233ed8a6c64097aafadd545ed24428).

**ACL HEADER**

1. 02 00 60 00 04 00 00 00
2. AclRevision (1 byte): 0x02
3. Reserved : 0x00
4. AclSize : 0x0060
5. AceCount : 0x0004
6. Reserved : 0x0000

**ACE Structure**

This is followed by the ACES in the ACL. For more information about the ACE structure, see section [2.4.4.1](#Section_628ebb1dc5094ea0a10f77ef97ca4586).

In this example, there are four ACEs for the DACL.

1. (A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)

First, look at the first access control entry (ACE) as an example. "(A;CIOI;GRGX;;;BU)" maps to the following in the binary structure (in little-endian order).

1. 00 03 18 00 00 00 00 a0 01 02 00 00 00 00 00 05-20 00 00 00 21 02 00 00

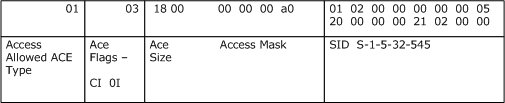


Figure 8: ACE field offsets

**Owner**

The **owner** begins at offset 0x90. In this example, owner is set to "BA" (Built-in Admin).



Figure 9: ACE owner field offsets example

**Group**

The **group** begins at offset 0xA0. In this example, group is set to "BA" (Built-in Admin).



Figure 10: ACE group field offsets example

### Token/Authorization Context

For a server implementation of an authenticated protocol, the result of the authentication produces a variety of data. Some of the data is related to the authentication protocol, such as keys for encrypted communication, and is covered in the relevant authentication protocol specification. Additionally, after the identity of the client is determined, additional data corresponding to authorization of the client to the server is derived. This additional information can be from the domain controller, server-local information, or a combination of the two, depending on implementation choices. This additional information is termed an authorization context.

The authorization context, also referred to as a Token, is a collection of the groups associated with the client principal, as well as additional optional policy information. The authorization context is central to determining access through the evaluation of a security descriptor, as shown in section [2.5.3](#Section_7e05ef44a9c4436aa38054ab92ea2f4b). Note that the Token is never passed directly across the network; tokens are local information and the actual representation is up to the implementation. This Token is represented as an abstract data structure as follows:

* **Sids[]**: An array of [SIDs](#Section_78eb90131c3a4970ad1f2b1dad588a25) that indicate the SID of the user account, the SIDs of all groups to which the user belongs, and SIDs that indicate contextual information such as logon type. The Sids[] array always contains at least the SID of the account; it is an error to have an empty set. The order of the SIDs is not specified, nor is it required that the array be treated logically as a set of SIDs. For the purposes of this document, the SIDs can be considered instances of the [RPC\_SID](#Section_5cb97814a1c24215b7dc76d1f4bfad01) structure.
* **UserClaims[]**: An optional array of [CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#Section_21f2b5f0737645bbbc31eaa60841dbe9) (defined in section 2.4.10.1) which have been issued to the user. The UserClaims[] array can be empty. The order of the Claims is not specified or required.
* **LocalClaims[]**: An optional array of CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 (defined in section 2.4.10.1) which have been issued to the authenticated principal. The LocalClaims[] array can be empty. The order of the Claims is not specified or required.
* **Privileges[]**: An array of [LUIDs](#Section_48cbee2a079045f28269931d7083b2c3) that is a set of administrative or security-relevant privileges associated with this authorization context. A set of logical privileges associated with the user, the privileges are administrative or security relevant in nature. It might be convenient to an implementation to represent a privilege as a LUID.
* **DeviceSids[]**: An optional array of SIDs that indicate the SID of the account of the computer which the user is connecting from, the SIDs of all groups to which that computer account belongs, and SIDs that indicate contextual information such as logon type. If the DeviceSids[] array is present, it always contains at least the SID of the computer account. The order of the SIDs is neither specified nor required. For the purposes of this document, the SIDs can be considered instances of the RPC\_SID structure.
* **DeviceClaims[]**: An optional array of CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 (defined in section 2.4.10.1) which have been issued to the account of the computer which the user is connecting from. The DeviceClaims[] array can be empty. The order of the DeviceClaims is not specified or required.
* **UserIndex**: An unsigned \_\_int32 that is an index into the **Sids[]** array that indicates which SID is the SID that represents the user account.
* **OwnerIndex**: An unsigned \_\_int32 that is an index into the **Sids[]** array that indicates which SID to assign as the owner for new objects. This value is determined by local policy in an implementation-specific manner. Ownership is often used, by way of example, for accounting for file storage space on a file server. This value can be the same as the UserIndex attribute, but is not required to be; this allows, for example, quota or ownership of objects to be assigned to groups rather than individuals.[<90>](#Appendix_A_90" \o "Product behavior note 90)
* **PrimaryGroup**: An unsigned \_\_int32 that is an index into the **Sids[]** array that indicates which SID to use as the primary group of the user.
* **DefaultDACL**: A **DACL**, as defined in section [2.4.5](#Section_20233ed8a6c64097aafadd545ed24428), that can be applied to new objects when there is no parent security descriptor for inheritance and no explicit new security descriptor was supplied by the client.

An Authorization context can optionally include mandatory integrity information and policy. This is not required for all instances, and can depend on the ability of the authentication protocol used to carry the necessary information. If an implementation also chooses to implement mandatory integrity in the same way as Windows does, the following additional fields are necessary.

* **IntegrityLevelSID**: A separate SID, not used for general access decisions like the Sids[] array above, that indicates the mandatory integrity level of this principal.
* **MandatoryPolicy**: An unsigned \_\_int32, the access policy for principals with a mandatory integrity level lower than the object associated with the **SACL** that contains this [ACE](#Section_d06e5a81176e46c69cf79137aad4455e). The possible values of this field are the same as those specified for the **Policy** field of [TOKEN\_MANDATORY\_POLICY (section 2.4.8)](#Section_de8373ec206f4dc8b3fec638fed7b282).

**Note**  For more information about tokens in Windows, see [[MSDN-ACCTOKENS]](https://go.microsoft.com/fwlink/?LinkId=89949).

#### Token/Authorization Context Algorithms

##### GatherGroupMembershipForSystem

The GatherGroupMembershipForSystem function accepts an array of [**SIDs**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) and invokes GatherLocalGroupMembership, which in turn invokes GatherLocalGroupMembershipFromLocalDomain for the local account [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) and again for the built-in domain.

An array of SIDs is returned that includes all input SIDs and the SIDs for all local groups of which the input SIDs are members.

1. GatherGroupMembershipForSystem( InitialMembership, FinalMembership )
2. --
3. -- On entry InitialMembership is a non-empty array of SIDs
4. --
5. -- On exit FinalMembership is a array of SIDs
6. --
7. CALL GatherLocalGroupMembership ( InitialMembership, FinalMembership )
8. END\_SUBROUTINE

The *InitialMembership* and *FinalMembership* parameters are arrays of SIDs. This method is called by authentication protocols during the process of authentication (see [[MS-KILE]](%5bMS-KILE%5d.pdf#Section_2a32282edd484ad9a542609804b02cc9) section 3.4.5.3 and [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 3.1.5.

1. GatherLocalGroupMembership( InitialMembership, FinalMembership )
2. --
3. -- On entry
4. -- InitialMembership is a non-empty set of SIDs
5. --
6. -- On exit
7. -- FinalMembership is a set of SIDs
8. --
9. GatherLocalGroupMembershipFromLocalDomain( InitialMembership,
10. LocalDomainSid,
11. FinalMembership )
12. GatherLocalGroupMembershipFromLocalDomain( FinalMembership,
13. BuiltinDomainSid,
14. FinalMembership )
15. END\_SUBROUTINE
16. GatherLocalGroupMembershipFromLocalDomain( InitialMembership,
17. LimitingDomain,
18. FinalMembership )
19. --
20. -- On entry
21. -- InitialMembership is an array of SIDs
22. -- LimitingDomain is a domain SID
23. --
24. -- On exit
25. -- FinalMembership is an array of SIDs including any SID from InitialMembership
26. -- plus all SIDs of groups of which SIDs in InitialMembership are members.
27. --
28. Domain d is the domain in Local Domains with objectSid equal LimitingDomain
29. AdditionalMembership is a set of sids initially empty
30. Set FinalMembership equal to InitialMembership
31. FOR EACH GROUP g in d DO
32. FOR EACH SID m in g.members DO
33. FOR EACH SID s in InitialMembership DO
34. if m equals s
35. Set AdditionalMembership equal to the union of
36. AdditionalMembership and g.objectSid
37. END IF
38. END FOR
39. END FOR
40. END FOR
41. Set FinalMembership equal to the union of
42. InitialMembership and AdditionalMembership
43. END\_SUBROUTINE

##### AddPrivilegesToToken

The AddPrivilegesToToken function returns a token with privileges based on the local PrivilegeMapping array using the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) in the token passed to the function, as shown in the following pseudocode.

1. AddPrivilegesToToken( Token )
2. -- On entry
3. -- Token is an authorization context containing all sids that represent the security principal
4. FOR EACH SID s in Token DO
5. FOR EACH MAPPING mapping in PrivilegeMapping DO
6. IF mapping.SID equals s
7. Token.Privileges is a union of Token.Privileges and mapping.Privileges
8. END IF
9. END FOR
10. END FOR
11. END-SUBROUTINE

### Security Descriptor Algorithms

The security descriptor is the basis for specifying the security associated with an object. The client makes a request to the server that indicates a particular requested access, and the server that "owns" the object is responsible for verifying that a client has sufficient access to the object in order to open or manipulate the object. In order to create a server that maintains the same guarantees of authorization to clients, the access check algorithm has to produce the same results.

The algorithms are straightforward, but are best served by extracting certain support functions out of the main path of the algorithm for clarity. These support functions are documented in the first section.

**Note**  For more information about tokens in Windows, see [[MSDN-ACCTOKENS]](https://go.microsoft.com/fwlink/?LinkId=89949).

When creating new objects, the security descriptor from the parent container of the new object is used as the template for the security descriptor of the new object.

#### Support Functions

The following pseudo-functions are used in the main access check and new security descriptor algorithms below.

##### SidInToken

A support function, SidInToken, takes the authorization context, a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) (referenced below as the *SidToTest* parameter), and an optional *PrincipalSelfSubstitute* parameter, and returns TRUE if the **SidToTest** is present in the authorization context; otherwise, it returns FALSE. The well-known SID PRINCIPAL\_SELF, if passed as **SidToTest**, is replaced by the *PrincipalSelfSubstitute* SID prior to the examination of the authorization context.

Any plug-in replacement is required to use this exact algorithm, which is described using the pseudocode syntax as specified in [[DALB]](https://go.microsoft.com/fwlink/?LinkId=89842).

1. BOOLEAN SidInToken(
2. Token,
3. SidToTest,
4. PrincipalSelfSubstitute )
5. --
6. -- On entry
7. -- Token is an authorization context containing all SIDs
8. -- that represent the security principal
9. -- SidToTest, the SID for which to search in Token
10. -- PrincipalSelfSubstitute, a SID with which SidToTest may be
11. -- replaced
12. IF SidToTest is the Well Known SID PRINCIPAL\_SELF THEN
13. set SidToTest to be PrincipalSelfSubstitute
14. END IF
15. FOR EACH SID s in Token.Sids[] DO
16. IF s equals SidToTest THEN
17. return TRUE
18. END IF
19. END FOR
20. Return FALSE
21. END-SUBROUTINE

##### SidDominates

A support function, SidDominates, compares the mandatory integrity levels expressed in two SIDs. The function returns TRUE if the first SID dominates the second SID or is equal to the second SID, or FALSE if the first SID is subordinate to the second SID. This function can be used only on SIDs that encode integrity levels (the SID\_IDENTIFIER\_AUTHORITY field is SECURITY\_MANDATORY\_LABEL\_AUTHORITY); any other use is unsupported.

Any plug-in replacement is required to use this exact algorithm, which is described using the pseudocode syntax as specified in [[DALB]](https://go.microsoft.com/fwlink/?LinkId=89842).

1. BOOLEAN
2. SidDominates(
3. SID sid1,
4. SID sid2)
5. -- On entrance, both sid1 and sid2 MUST be SIDs representing integrity levels
6. -- as specified in section 2.4.4.11. Use of any other SID is a logic error.
7. -- On exit, a value of TRUE indicates that sid1 dominates or is equivalent to sid2.
8. -- A value of FALSE indicates that sid1 is dominated by sid2. Dominance in
9. -- this context is determination of the dominance of one integrity level over
10. -- another in a manner as broadly described, for example, in the Biba Integrity Model.
11. IF sid1 equals sid2 THEN
12. Return TRUE
13. END IF
14. -- If Sid2 has more SubAuthorities than Sid1, Sid1 cannot dominate.
15. IF sid2.SubAuthorityCount GREATER THAN sid1.SubAuthorityCount THEN
16. Return FALSE
17. END IF
18. --on entry, index is zero and is incremented for each iteration of the loop.
19. FOR each SubAuthority in sid1
20. IF sid1.SubAuthority[ index ] GREATER THAN or EQUAL TO sid2.SubAuthority[ index ] THEN
21. Return TRUE
22. END IF
23. END FOR
24. Return FALSE

##### GetScopedPolicySid

A support function, **GetScopedPolicySid**, locates the first non-inherit-only scoped policy ACE in the ACL passed in, if one is present, and returns the SID it contains. If one is not present, then NULL is returned.

Only the SID of the first non-inherit-only scoped policy ACE is returned and enforced, but inherit-only scoped policy ACEs are allowed to be present in the ACL, because they might be inherited and applied to child objects.

1. SID
2. GetScopedPolicySid(
3. ACL Sacl)
4. --
5. -- On entry
6. -- Sacl is the Sacl from the security descriptor used for Access Check.
7. --
8. FOR EACH ACE in Sacl DO
9. IF ACE.Type is SYSTEM\_SCOPED\_POLICY\_ID\_ACE THEN
10. IF ACE.AceFlags does not contain INHERIT\_ONLY\_ACE flag THEN
11. Return ACE.Sid
12. END IF
13. END FOR
14. Return NULL
15. END-SUBROUTINE

##### GetCentralizedAccessPolicy

A support function, GetCentralizedAccessPolicy, determines if there is a central access policy and, if so, returns it based on the policy SID in the SACL. If no policy matches the policy SID, the function returns an implementation-specific local recovery policy.[<91>](#Appendix_A_91" \o "Product behavior note 91)

1. CentralizedAccessPolicy
2. GetCentralizedAccessPolicy(
3. ACL Sacl)
4. --
5. -- On entry
6. -- Sacl is the Sacl from the security descriptor used for Access Check.
7. --
8. -- Returns
9. -- NULL - there is no policy
10. -- The policy from the configuration if one exists and matches the scoped SID
11. -- The default (recovery) policy if none match the scoped SID
12. --
13. Dim SID CentralizedAccessPolicySid
14. Dim CentralAccessPolicy CentralizedAccessPolicy
15. IF No central access policy is present in the configuration THEN
16. return NULL
17. END IF
18. IF SACL is not NULL THEN
19. CALL GetScopedPolicySid(SACL) returning CentralizedAccessPolicySid
20. IF CentralizedAccessPolicySid is not NULL THEN
21. Get CentralizedAccessPolicy using CentralizedAccessPolicySid
22. IF CentralizedAccessPolicy is NULL THEN
23. Set CentralizedAccessPolicy to RecoveryCentralizedAccessPolicy
24. END IF
25. END IF
26. END IF
27. return CentralizedAccessPolicy
28. END-SUBROUTINE

##### EvaluateAceCondition

A support function, **EvaluateAceCondition**, evaluates the ACE **ApplicationData** field utilizing the authorization information passed in as parameters. The **ApplicationData** is stored in binary format in Postfix notation. In this notation, every operator follows all of its required operands and the notion of parenthesis is built into the construction of this data.

The evaluation takes place by scanning the **ApplicationData** from left to right. Operands are pushed onto the stack, and when an operator is encountered, the appropriate items are popped off the stack. The result of the operation is then pushed back onto the stack.

1. INT32 Result
2. AuthzBasepEvaluateAceCondition(
3. TOKEN Token,
4. ACL Sacl,
5. BYTE[] ApplicationData,
6. ULONG ApplicationDataSize )
7. --
8. -- On entry
9. -- Token - the Authz context or NT Token representing the user.
10. -- Sacl – SecurityDescriptor SACL field containting ACE’s with resource claims.
11. -- ApplicationData – the condition to be evaluated.
12. -- ApplicationDataSize – the length of the condition passed in.
13. -- Result - The result of the evaluation. 1: true; 0: false; -1: unknown.
14. "unknown" is returned when the Token/Sacl doesn't contain enough information
15. to evaluate the ApplicationData.
16. Dim StackElement
17. {
18. STRING Type
19. -- Could be "User Attribute" from Token
20. -- or "Device Attribute" from the Token
21. -- or "Local Attribute" from the Token
22. -- or "Resource Attribute" from the Sacl
23. -- or a "Literal" from ApplicationData stream
24. -- or a processed "Result Value"
25. CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 Operand
26. -- Unprocessed attribute or literal data
27. INT32 Result
28. -- Processed result of an operator evaluation
29. }
30. Dim StackElement ResultStack[]
31. Dim WCHAR AttributeName
32. Dim BYTE TokenType
33. Set StackPos to 0
34. IF ApplicationData does not begin with ACE\_CONDITION\_SIGNATURE THEN
35. Set Result to -1
36. Return Result
37. END IF
38. Set i to size of ACE\_CONDITION\_SIGNATURE
39. WHILE i less than ApplicationDataSize
40. - Begin scanning the ApplicationData byte stream.
41. Set TokenType to ApplicationData[i]
42. CASE TokenType OF
43. -- Byte codes for attributes are defined in Byte-Code column in the table in section 2.4.4.17.8.
44. -- ATTRIBUTE TOKEN
45. CASE 0xf8-0xfb:
46. -- Extraction rules for these byte codes are defined in Token Data Encoding
47. -- column in the table in section 2.4.4.17.8.
48. Set AttributeName to unicode string extracted from ApplicationData stream
49. IF TokenType equals 0xfa THEN
50. -- Resource attributes
51. CALL LookupAttributeInSacl(AttributeName, Sacl)
52. ELSE
53. -- User/Device/Legacy attributes
54. CALL LookupAttributeInToken(AttributeName, Token, TokenType)
55. ENDIF
57. Set TempOperand to return value of above lookup
58. CALL PushStackOperand(ResultStack, StackPos, TokenType, TempOperand)
59. -- Bytes consumed for these byte codes are defined in Token Data Encoding column
60. -- in the table in section 2.4.4.17.8.
61. Increment i by ApplicationData consumed + 1
63. -- Byte codes for literals are defined in Byte-code column in the table in section
64. -- 2.4.4.17.5
65. -- LITERALS
66. CASE 0x01-0x04,0x10,0x18,0x50,0x51:
67. -- Extraction rules for these byte codes are defined in Token Data Encoding column in
68. -- the table in section 2.4.4.17.5
69. Set TempOperand to extracted literal from ApplicationData stream
70. CALL PushStackOperand(ResultStack, StackPos, "Literal", TempOperand)
71. -- Bytes consumed for these byte codes are defined in Token Data Encoding column
72. -- in the table in section 2.4.4.17.5
73. Increment i by ApplicationData consumed + 1
74. -- Byte codes for unary logical operators are defined in Byte-code column in the
75. -- Unary Logical Operators table in section 2.4.4.17.7
76. -- UNARY LOGICAL OPERATORS
77. CASE 0xa2,0x87,0x8d:
78. -- Requires 1 operand
79. CALL PopStack(ResultStack, StackPos)
80. Set Operand to popped stack item
81. -- Validation and evaluation rules for these byte codes are defined in Processing
82. -- column in the Unary Logical Operators table in section 2.4.4.17.7
83. Set TempResult to evaluation of Operand for this operator
84. -- Push the result onto the stack
85. CALL PushStackResult(ResultStack, StackPos, TempResult)
86. -- Bytes consumed for these operators is 1
87. Increment i by 1
88. -- BINARY LOGICAL OPERATORS
89. -- Byte codes for binary logical operators are defined in Byte-code column in the
90. -- Binary Logical Operators table in section 2.4.4.17.7
91. CASE 0xa0,0xa1:
92. -- Requires 2 operands
93. CALL PopStack(ResultStack, StackPos)
94. Set RHS to popped stack item
95. CALL PopStack(ResultStack, StackPos)
96. Set LHS to popped stack item
97. -- Validation and evaluation rules for these byte codes are defined in Processing
98. -- column in the Binary Logical Operators table in section 2.4.4.17.7
99. Set TempResult to evaluation of LHS & RHS for this operator
100. -- Push the result onto the stack
101. CALL PushStackResult(ResultStack, StackPos, TempResult)
102. -- Bytes consumed for these operators is 1
103. Increment i by 1
104. -- Byte codes for unary relational operators are defined in Byte-code column in the
105. -- Unary Relational Operators table in section 2.4.4.17.6
106. -- UNARY RELATIONAL OPERATORS
107. CASE 0x89-0x8c, 0x90-0x93:
108. -- Requires 1 operand
109. CALL PopStack(ResultStack, StackPos)
110. Set Operand to popped stack item
111. -- Validation and evaluation rules for these byte codes are defined in Processing
112. -- column in the Unary Relational Operators table in section 2.4.4.17.6
113. Set TempResult to evaluation of Operand for this operator
114. -- Push the result onto the stack
115. CALL PushStackResult(ResultStack, StackPos, TempResult)
116. -- Bytes consumed for these operators is 1
117. Increment i by 1
118. -- Byte codes for binary relational operators are defined in Byte-code column in the
119. -- Binary Relational Operators table in section 2.4.4.17.6
120. -- BINARY RELATIONAL OPERATORS
121. CASE 0x80-0x86,0x88,0x8e,0x8f:
122. -- Requires 1 operand
123. CALL PopStack(ResultStack, StackPos)
124. Set RHS to popped stack item
125. CALL PopStack(ResultStack, StackPos)
126. Set LHS to popped stack item
127. -- Validation and evaluation rules for these byte codes are defined in Processing
128. -- column in the Binary Relational Operators table in section 2.4.4.17.6
129. Set TempResult to evaluation of LHS & RHS for this operator
130. -- Push the result onto the stack
131. CALL PushStackResult(ResultStack, StackPos, TempResult)
132. -- Bytes consumed for these operators is 1
133. Increment i by 1
134. DEFAULT CASE
135. Set Result to -1
136. Return Result
137. END CASE
138. END WHILE
139. IF StackPos is equal to 1 THEN
140. Set Result to ResultStack[0].Result
141. ELSE
142. Set Result to -1
143. ENDIF
144. Return Result
145. END-SUBROUTINE

##### LookupAttributeInToken

A support function, **LookupAttributeInToken**, locates an attribute in the token based on the *AttributeName* passed in, if one is present. If one is not present then NULL is returned.

1. CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1
2. LookupAttributeInToken (
3. WCHAR AttributeName,
4. TOKEN Token,
5. BYTE Source
6. )
7. --
8. -- On entry
9. -- AttributeName is the Unicode string attribute.
10. -- Token is the Authz context or NT Token representing the user
11. -- Source indicates which section of the token to look for the attributes.
12. Dim CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 LookupList[]
13. IF Source is equal to 0xf8 THEN
14. Set LookupList to Token.LocalClaims
15. ENDIF
16. IF Source is equal to 0xf9 THEN
17. Set LookupList to Token.UserClaims
18. ENDIF
19. IF Source is equal to 0xfb THEN
20. Set LookupList to Token.DeviceClaims
21. ENDIF
22. FOR EACH Attribute in LookupList DO
23. IF Attribute.Name equals AttributeName THEN
24. Return Attribute
25. END IF
26. END FOR
27. Return NULL
28. END-SUBROUTINE

##### LookupAttributeInSacl

A support function, **LookupAttributeInSacl**, locates an attribute in the Sacl based on the *AttributeName* passed in, if one is present. If one is not present then NULL is returned.

1. CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1
2. LookupAttributeInSacl (
3. WCHAR AttributeName,
4. ACL Sacl
5. )
6. --
7. -- On entry
8. -- AttributeName is the Unicode string attribute.
9. -- Sacl containing the attribute information.
10. Dim CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 SaclAttribute
11. FOR EACH ACE in Sacl DO
12. IF ACE.Type is SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE\_TYPE THEN
13. -- Refer section 2.4.4.15
14. Set TempAttribute to Ace.AttributeData
15. IF TempAttribute.Name equals AttributeName THEN
16. Return TempAttribute
17. END IF
18. END IF
19. END FOR
20. Return NULL
21. END-SUBROUTINE

##### PushStackOperand

A support function, **PushStackOperand**, pushes the input Operand on the stack.

1. PushStackOperand (
2. STACK ResultStack,
3. INT32 StackPos,
4. BYTE Type,
5. CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 TempOperand
6. )
7. --
8. -- On entry
9. -- ResultStack is the stack.
10. -- StackPos is the stack position
11. -- Type is the type of operand, either attribute type or literal
12. -- TempOperand is the value to be stored on the stack
13. Set ResultStack[StackPos].Operand to TempOperand
14. Set ResultStack[StackPos].Type to Type
15. Increment StackPos by 1
16. END-SUBROUTINE

##### PushStackResult

A support function, **PushStackResult**, pushes the input Result on the stack.

1. PushStackResult (
2. STACK ResultStack,
3. INT32 StackPos,
4. INT32 ResultValue
5. )
6. --
7. -- On entry
8. -- ResultStack is the stack.
9. -- StackPos is the stack position
10. -- ResultValue is the result value to be stored on the stack
11. Set ResultStack[StackPos].Result to ResultValue
12. Set ResultStack[StackPos].Type to "Result Value"
13. Increment StackPos by 1
14. END-SUBROUTINE

##### PopStack

A support function, **PopStack**, pops the topmost operand from the stack.

1. STACKELEMENT
2. PopStack (
3. STACK ResultStack,
4. INT32 StackPos
5. )
6. --
7. -- On entry
8. -- ResultStack is the stack.
9. -- StackPos is the stack position
10. IF StackPos equals 0 THEN
11. Return NULL
12. END IF
13. Decrement StackPos by 1
14. Return ResultStack[StackPos]
15. END-SUBROUTINE

#### Access Check Algorithm Pseudocode

In overview, the Access Check algorithm takes an access request and a security descriptor. It iterates through the **DACL** of the security descriptor, processing each [ACE](#Section_d06e5a81176e46c69cf79137aad4455e). If the ACE contains a [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25) that is also in the Token authorization context, then the ACE is processed, otherwise it is skipped. If an ACE grants access to that SID, then those access rights from the Access Request Mask are considered satisfied, and removed from the mask. If the ACE denies access to that SID, and the access rights in the ACE are present in the request mask, the whole request is denied. At the end of the algorithm, if there are any access rights still pending in the Access Request Mask, then the request is considered denied.

There are two noteworthy configurations of the security descriptor in light of the access check algorithm: an empty **DACL**, and a NULL (or absent) **DACL**. No **DACL** in the security descriptor implies that there is no policy in place to govern access to the object; any access check will succeed. An empty **DACL**, where the **DACL** is marked as being present but contains no ACEs, means that no principal can gain access to the object, except through the implied access of the owner.

If the access request is MAXIMUM\_ALLOWED, the algorithm operates in a different mode. It iterates through every ACE in the **DACL** of the security descriptor, remembering which access rights were granted or denied for each ACE. After all ACEs have been examined, the complete set of grantable access rights is computed and returned via the *GrantedAccess* parameter (described later in this section).

Note that the use of MAXIMUM\_ALLOWED is not recommended; instead, callers can request the specific minimum level of access required to accomplish their requirements.

The detailed processing of the list is as follows.

On entrance:

* SecurityDescriptor: [SECURITY\_DESCRIPTOR](#Section_7d4dac059cef4563a058f108abecce1d) structure that is assigned to the object.
* Token: Authorization context as described above.
* Access Request mask: Set of permissions requested on the object.
* Object Tree: An array of OBJECT\_TYPE\_LIST structures representing a hierarchy of objects for which to check access. Each node represents an object with three values: A [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that represents the object itself; a value called Remaining, which can be zero, and which specifies the user rights requests for that node that have not yet been satisfied; and a value called Level, which indicates the level of the object type in the hierarchy.
* PrincipalSelfSubst SID: A SID that logically replaces the SID in any ACE that contains the well-known PRINCIPAL\_SELF SID. It can be null.
* GrantedAccess: An optional [ACCESS\_MASK](#Section_7a53f60ee7304dfebbe9b21b62eb790b) output parameter used when the *Access Request Mask* parameter equals MAXIMUM\_ALLOWED. Upon return this parameter contains the set of permissions granted to *Token* by the *SecurityDescriptor*.

1. STATUS\_CODE
2. EvaluateTokenAgainstDescriptor(
3. TOKEN Token,
4. SECURITY\_DESCRIPTOR SecurityDescriptor,
5. ACCESS\_MASK Access\_Request\_mask,
6. OBJECT\_TYPE\_LIST Object Tree,
7. Sid PrincipalSelfSubstitute,
8. [out] ACCESS\_MASK GrantedAccess)
9. Dim OBJECT\_TYPE\_LIST LocalTree
10. Dim ULONG Result
11. Set DACL to SecurityDescriptor Dacl field
12. Set SACL to SecurityDescriptor Sacl field
13. Set RemainingAccess to Access Request mask
14. Set AllowedAccesses to 0
15. Set DeniedAccesses to 0
16. Set MaxAllowedMode to FALSE
17. IF RemainingAccess contains ACCESS\_SYSTEM\_SECURITY access bit THEN
18. IF Token.Privileges contains SeSecurityPrivilege THEN
19. Remove ACCESS\_SYSTEM\_SECURITY access bit from RemainingAccess
20. Set GrantedAccess to GrantedAccess or ACCESS\_SYSTEM\_SECURITY
21. IF RemainingAccess to 0 THEN
22. Return success
23. Else
24. ELSE
25. Set GrantedAccess to 0
26. Return access\_denied
27. END IF
28. END IF
29. IF RemainingAccess contains WRITE\_OWNER access bit and Token.Privileges is not NULL THEN
30. IF Token.Privileges contains SeTakeOwnershipPrivilege THEN
31. Remove WRITE\_OWNER access bit from RemainingAccess
32. Set GrantedAccess to GrantedAccess or WRITE\_OWNER
33. END IF
34. END IF
35. -- the owner of an object is always granted READ\_CONTROL and WRITE\_DAC.
36. CALL SidInToken(Token, SecurityDescriptor.Owner, PrincipalSelfSubst)
37. IF SidInToken returns True THEN
38. IF DACL does not contain ACEs from object owner THEN
39. Remove READ\_CONTROL and WRITE\_DAC from RemainingAccess
40. Set GrantedAccess to GrantedAccess or READ\_CONTROL or WRITE\_OWNER
41. END IF
42. END IF
43. -- Support for MAXIMUM\_ALLOWED
44. IF RemainingAccess contains MAXIMUM\_ALLOWED access bit THEN
45. Set MaxAllowedMode to TRUE
46. END IF
47. IF Object Tree is not NULL THEN
48. Set LocalTree to Object Tree
49. -- node is of type OBJECT\_TYPE\_LIST
50. FOR each node in LocalTree DO
51. Set node.Remaining to RemainingAccess
52. END FOR
53. END IF
54. FOR each ACE in DACL DO
55. IF ACE.AceFlags does not contain INHERIT\_ONLY\_ACE THEN
57. CASE ACE.Type OF
58. CASE Allow Access:
59. CALL SidInToken( Token, ACE.Sid, and PrincipalSelfSubst )
60. IF SidInToken returns True THEN
61. IF MaxAllowedMode equals TRUE THEN
62. Set AllowedAccesses to AllowedAccesses or ACE.AccessMask
63. Set GrantedAccess to GrantedAccess or ACE.AccessMask
64. ELSE
65. Remove ACE.AccessMask from RemainingAccess
66. Set GrantedAccess to GrantedAccess or(RemainingAccess and
67. ACE.AccessMask)
68. FOR each node in LocalTree DO
69. Remove ACE.AccessMask from node.Remaining
70. END FOR
71. END IF
72. END IF
74. CASE Deny Access:
75. IF ACE.AccessMask equals 0 returns True THEN Break
76. CALL SidInToken( Token, ACE.Sid, PrincipalSelfSubst )
77. IF SidInToken returns True THEN
78. IF MaxAllowedMode equals TRUE THEN
79. Set DeniedAccesses to DeniedAccesses or ACE.AccessMask
80. ELSE
81. IF any bit of RemainingAccess is in ACE.AccessMask THEN
82. Set GrantedAccess to 0
83. Return access\_denied
84. END IF
85. END IF
86. END IF
88. CASE Object Allow Access:
89. CALL SidInToken( Token, ACE.Sid, PrincipalSelfSubst )
90. IF SidInToken returns True THEN
91. IF ACE.Object is contained in LocalTree THEN
92. Locate node n in LocalTree such that
93. n.GUID is the same as ACE.Object
94. Remove ACE.AccessMask from n.Remaining
95. FOR each node ns such that ns is a descendent of n DO
96. Remove ACE.AccessMask from ns.Remaining
97. END FOR
98. FOR each node np such that np is an ancestor of n DO
99. Set np.Remaining to np.Remaining or np-1.Remaining
100. -- the 'or' above is a logical bitwise OR operator. For
101. -- Some uses (like Active Directory), a hierarchical list
102. -- of types can be passed in; if the requestor is granted
103. -- access to a specific node, this will grant access to
104. -- all its children. The preceding lines implement this by
105. -- removing, from each child, the permissions just found for
106. -- the parent. The change is propagated upwards in
107. -- the tree: once a permission request has been satisfied
108. -- we can tell the next-higher node that we do not need
109. -- to inherit it from the higher node (we already have it
110. -- in the current node). And since we must not blindly
111. -- replace the parent's RemainingAccess, we BIT\_OR the
112. -- parent's RemainingAccess with the current node's. This
113. -- way, if the parent needs, say, READ\_CONTROL, and the
114. -- current node was just granted that, the parent's
115. -- RemainingAccess still contains this bit since satisfying
116. -- the request at a lower level does nothing to affect
117. -- the higher level node. Active Directory has its own
118. -- checking rules--see [MS-ADTS] section 3.1.1.4.3.
120. END FOR
121. END IF
122. END IF
124. CASE Object Deny Access:
125. CALL SidInToken( Token, ACE.Sid, PrincipalSelfSubst )
126. IF SidInToken returns True THEN
127. Locate node n in LocalTree such that
128. n.GUID is the same as ACE.Object
129. IF n exists THEN
130. If any bit of n.Remaining is in ACE.AccessMask THEN
131. Set GrantedAccess to 0
132. Return access\_denied
133. END IF
134. END IF
135. END IF
136. CASE Allow Access Callback Ace:
137. EvaluateAceCondition(Token,
138. Sacl,
139. ApplicationData,
140. ApplicationDataSize) returning Result
141. IF Result is 1 THEN
142. IF (SidInToken(Token, ACE.Sid, PrincipalSelfSubst)) THEN
143. IF MaxAllowedMode equals TRUE THEN
144. Set GrantedAccess to GrantedAccess or ACE.AccessMask
145. Set AllowedAccesses to AllowedAccesses or ACE.AccessMask
146. ELSE
147. Remove ACE.AccessMask from RemainingAccess
148. SET n = root node of object tree
149. FOR each node np such that np is an ancestor of n DO
150. Set np.Remaining to np.Remaining or np-1.Remaining
151. -- the 'or' above is a logical bitwise OR operator. For
152. -- Some uses (like Active Directory), a hierarchical list
153. -- of types can be passed in; if the requestor is granted
154. -- access to a specific node, this will grant access to
155. -- all children. The preceding lines implement this by
156. -- removing, from each child, the permissions just found for
157. -- the parent. The change is propagated upwards in
158. -- the tree: once a permission request has been satisfied
159. -- we can tell the next-higher node that we do not need
160. -- to inherit it from the higher node (we already have it
161. -- in the current node). And since we must not blindly
162. -- replace the parent's RemainingAccess, we BIT\_OR the
163. -- parent's RemainingAccess with the current node's. This
164. -- way, if the parent needs, say, READ\_CONTROL, and the
165. -- current node was just granted that, the parent's
166. -- RemainingAccess still contains this bit since satisfying
167. -- the request at a lower level does nothing to affect
168. -- the higher level node.
169. END FOR
170. END IF
171. END IF
172. END IF
173. END CASE
174. END IF
175. END FOR
176. IF MaxAllowedMode equals TRUE THEN
177. -- The not operator below is a bit-wise operator
178. Set GrantedAccess to AllowedAccesses and (not DeniedAccesses)
179. IF GrantedAccess not equals 0 THEN
180. Return success
181. ElSE
182. Return access\_denied
183. END IF
184. SET GrantedAccess to 0
185. IF RemainingAccess to 0 THEN
186. Return success
187. Else
188. Return access\_denied
189. END IF
190. END-SUBROUTINE
191. STATUS\_CODE
192. AccessCheck(
193. TOKEN Token,
194. SECURITY\_DESCRIPTOR SecurityDescriptor,
195. ACCESS\_MASK Access Request mask,
196. OBJECT\_TYPE\_LIST Object Tree,
197. Sid PrincipalSelfSubstitute,
198. [out] ACCESS\_MASK GrantedAccess)
199. Dim CentralAccessPolicy CentralizedAccessPolicy
200. Dim SECURITY\_DESCRIPTOR CaprSecurityDescriptor
201. Dim SECURITY\_DESCRIPTOR StagedCaprSecurityDescriptor
202. Dim ACCESS\_MASK DesiredAccess
203. Dim ACCESS\_MASK CentralAccessPolicyEffectiveAccess
204. Dim ACCESS\_MASK CentralAccessPolicyEntryEffectiveAccess
205. Dim ACCESS\_MASK CentralAccessPolicyStagedAccess
206. Dim ACCESS\_MASK CentralAccessPolicyEntryStagedAccess
207. Dim ULONG Result
208. Dim STATUS\_CODE Status
210. Set DACL to SecurityDescriptor Dacl field
211. Set SACL to SecurityDescriptor Sacl field
212. Set RemainingAccess to Access Request mask
213. Set AllowedAccesses to 0
214. Set DeniedAccesses to 0
215. Set DesiredAccess to Access Request mask
216. CALL EvaluateTokenAgainstDescriptor(Token,
217. SecurityDescriptor,
218. DesiredAccess,
219. Object Tree,
220. PrincipalSelfSubstitute,
221. GrantedAccess) returning Status
222. IF Status is access\_denied THEN
223. return Status
224. END IF
225. CALL GetCentralizedAccessPolicy(SACL) returning CentralizedAccessPolicy
226. IF CentralizedAccessPolicy is not NULL THEN
227. Set CentralAccessPolicyEffectiveAccess to GrantedAccess
228. Set CentralAccessPolicyStagedAccess to GrantedAccess
229. FOR each CentralAccessPolicyRule in CentralAccessPolicy.RulesList
230. EvaluateAceCondition(Token,
231. SACL,
232. AppliesTo,
233. AppliesToSize) returning Result
234. IF Result is not 1 THEN
235. GOTO NextRule
236. END IF
237. Copy SecurityDescriptor to CaprSecurityDescriptor
238. Set CaprSecurityDescriptor.DACL to
239. CentralAccessPolicyRule.EffectiveCentralAccessPolicy.AccessCondition.DACL
240. EvaluateTokenAgainstDescriptor
241. (Token,
242. CaprSecurityDescriptor,
243. DesiredAccess,
244. NULL,
245. PrincipalSelfSubstitute,
246. CentralAccessPolicyEntryEffectiveAccess)
247. -- The and operator below is a bit-wise operator
248. Set CentralAccessPolicyEffectiveAccess to
249. CentralAccessPolicyEffectiveAccess and CentralAccessPolicyEntryEffectiveAccess
250. -- StagingLocalPolicyEnabled = True if MS-GPAC ADM variable
251. -- "System Advanced Audit Policy" (MS-GPAC section 3.2.1.1) contains the GUID
252. -- for "Central Access Policy Staging" as specified in MS-GPAC section 2.2.1.2
253. IF IfStagingLocalPolicyEnabled THEN
254. Copy SecurityDescriptor to StagedCaprSecurityDescriptor
255. Set StagedCaprSecurityDescriptor.DACL to
256. CentralAccessPolicyRule.StagedCentralAccessPolicy.AccessControl.DACL
257. EvaluateTokenAgainstDescriptor
258. (Token,
259. StagedCaprSecurityDescriptor,
260. DesiredAccess,
261. NULL,
262. PrincipalSelfSubstitute,
263. CentralAccessPolicyEntryStagedAccess)
264. -- The and operator below is a bit-wise operator
265. Set CentralAccessPolicyStagedAccess to CentralAccessPolicyStagedAccess
266. and CentralAccessPolicyEntryStagedAccess
267. ELSE IF CentralAccessPolicyEffectiveAccess is 0 THEN
268. Set GrantedAccess to 0
269. return access\_denied
270. END IF
271. NextRule:
272. END FOR
273. IF CentralAccessPolicyEffectiveAccess is not equal to
274. CentralAccessPolicyStagedAccess THEN
275. -- Log the difference between the Effective and Staged Access
276. END IF
277. -- The "not" and "and" operator below is a bit-wise operator
278. Set AllowedAccess to AllowedAccess and CentralAccessPolicyEffectiveAccess
279. Set RemainingAccess to DesiredAccess and not CentralAccessPolicyEffectiveAccess
280. FOR each node in Object Tree DO
281. Set node.Remaining to RemainingAccess
282. END FOR
283. ELSE
284. Return success
285. END IF
286. IF MaxAllowedMode equals TRUE THEN
287. -- The not operator below is a bit-wise operator
288. Set GrantedAccess to AllowedAccesses and (not DeniedAccesses)
289. IF GrantedAccess is 0 THEN
290. Return access\_denied
291. Else
292. Return success
293. END IF
294. END IF
295. SET GrantedAccess to 0
297. IF RemainingAccess is 0 THEN
298. Return success
299. Else
300. Return access\_denied
301. END IF
302. END-SUBROUTINE

#### MandatoryIntegrityCheck Algorithm Pseudocode

The Windows integrity mechanism extends the security architecture by defining a new [ACE](#Section_d06e5a81176e46c69cf79137aad4455e) type to represent an integrity level in an object's security descriptor.[<92>](#Appendix_A_92" \o "Product behavior note 92) The new ACE represents the object integrity level. An integrity level is also assigned to the security access token when the access token is initialized. The integrity level in the access token represents a subject integrity level. The integrity level in the access token is compared against the integrity level in the security descriptor when the security reference monitor performs an access check. The Access Check algorithm determines what access rights are allowed to a securable object. Windows restricts the allowed access rights depending on whether the subject's integrity level is equal to, higher than, or lower than the object, and depending on the integrity policy flags in the new access control ACE. The security subsystem implements the integrity level as a mandatory label to distinguish it from the discretionary access (under user control) that DACLs provide.

The MandatoryIntegrityCheck Algorithm examines the global Mandatory Integrity Check policy and applies the policy to the passed token and security descriptor of a securable object. It determines the set of access bits that can be granted by the DACL to a security principal.

1. --On entrance to the MandatoryIntegrityCheck Algorithm
2. -- IN IntegrityLevelSID Mandatory Integrity SID of the Token
3. -- IN AceIntegritySID Mandatory Integrity SID of the Security Descriptor of the securable object
4. -- OUT MandatoryInformation MANDATORY\_INFORMATION value, output of the MandatoryIntegrityCheck
5. -- Algorithm describing the allowable bits for the caller
6. -- Token Security Context for the calling security principal
7. -- IN ObjectSecurityDescriptor SECURITY\_DESCRIPTOR structure that is assigned to the object
8. Dim Boolean TokenDominates
9. -- TokenDominates value indicating that the IntegrityLevelSID is higher than the AceIntegritySID
10. Dim TOKEN\_MANDATORY\_POLICY TokenPolicy
11. Set TokenPolicy to Token.MandatoryPolicy field
12. Dim SYSTEM\_MANDATORY\_LABEL\_ACE ObjectIntegrityACE
13. -- Find the Manadatory ACE of ObjectSecurityDescriptor in the Sacl
14. Call FindAceByType WITH ObjectSecurityDescriptor.Sacl,
15. SYSTEM\_MANDATORY\_LABEL\_ACE\_TYPE, 0
16. RETURNING MandatoryACE, FoundIndex
17. Set ObjectIntegrityACE = MandatoryACE
18. Dim ACCESS\_MASK ObjectIntegrityAceMask
19. --Set ObjectIntegrityAceMask to the Access Mask field of the
20. --SYSTEM\_MANDATORY\_LABEL\_ACE of the ObjectSecurityDescriptor
21. Set ObjectIntegrityAceMask to MandatoryACE.Mask
22. IF TokenPolicy.Policy EQUAL TOKEN\_MANDATORY\_POLICY\_OFF OR
23. TokenPolicy.Policy EQUAL TOKEN\_MANDATORY\_POLICY\_NEW\_PROCESS\_MIN THEN
24. Set MandatoryInformation.AllowedAccess to GENERIC\_ALL
25. Return success
26. END IF
27. Dim PACE\_HEADER ACE
28. Set ACE to the ObjectSecurityDescriptor SACL of the
29. SYSTEM\_MANDATORY\_LABEL\_ACE
30. Dim ACCESS\_MASK AceMask
31. Set AceMask to zero
32. IF (ACE.AceFlags does not contain INHERIT\_ONLY\_ACE) THEN
33. Set AceMask to ObjectIntegrityAceMask
34. Set AceIntegritySID to the SID whose first DWORD is given by
35. ObjectIntegrityACE SidStart
36. ELSE
37. Set AceMask to SYSTEM\_MANDATORY\_LABEL\_NO\_WRITE\_UP
38. --The DefaultMandatorySID is derived from policy managed in an
39. --implementation-specific manner. The SID for ML\_MEDIUM is used by
40. --Windows S-1-16-8192.
41. Set AceIntegritySID to DefaultMandatorySID
42. END IF
43. IF CALL CompareSid (IntegrityLevelSID, AceIntegritySID,)returns TRUE
44. THEN
45. Set TokenDominates to TRUE
46. ELSE
47. CALL SidDominates (IntegrityLevelSID, AceIntegritySID)
49. IF SidDominates returns TRUE THEN
50. Set TokenDominates to TRUE
51. ELSE
52. Set TokenDominates to FALSE
53. END IF
54. END IF
55. IF TokenPolicy EQUAL TOKEN\_MANDATORY\_POLICY\_NO\_WRITE\_UP THEN
56. Add GENERIC\_READ to MandatoryInformation.AllowedAccess
57. Add GENERIC\_EXECUTE to MandatoryInformation.AllowedAccess
58. IF TokenDominates is TRUE THEN
59. Add GENERIC\_WRITE to MandatoryInformation.AllowedAccess
60. END IF
61. END IF
62. IF TokenDominates is FALSE THEN
63. IF AceMask & SYSTEM\_MANDATORY\_LABEL\_NO\_READ\_UP THEN
64. Remove GENERIC\_READ from MandatoryInformation.AllowedAccess
65. END IF
67. IF AceMask & SYSTEM\_MANDATORY\_LABEL\_NO\_WRITE\_UP THEN
68. Remove GENERIC\_WRITE from MandatoryInformation.AllowedAccess
69. END IF
71. IF AceMask & SYSTEM\_MANDATORY\_LABEL\_NO\_EXECUTE\_UP THEN
72. Remove GENERIC\_EXECUTE from MandatoryInformation.AllowedAccess
73. END IF
74. END IF
75. -- SeRelabelPrivilege see [MS-LSAD] 3.1.1.2.1 Privilege Data Model
76. IF Token.Privileges contains SeRelabelPrivilege THEN
77. Add WRITE\_OWNER to MandatoryInformation.AllowedAccess
78. END IF
79. ---------------------------
80. BOOLEAN CompareSid (
81. SID Sid1,
82. SID Sid2 )
83. -- On entrance, both sid1 and sid2 MUST be SIDs representing integrity levels
84. IF Sid1 Revision does not equal Sid2 Revision
85. return (false);
86. END IF
88. Dim integer SidLength = 0;
89. SidLength = (8 + (4 \*(Sid1 SubAuthorityCount)))
90. -- Compare the Sidlength bytes of Sid1 to Sidlength bytes of Sid2
91. -- Return TRUE if Sid1 equals Sid2
92. return(!memcmp( Sid1, Sid2, SidLength))

##### FindAceByType

The FindAceByType support function finds an [ACE](#Section_d06e5a81176e46c69cf79137aad4455e) based on the given ACE type and index and returns it along with the index of its location.

**Parameters**

* *Acl*: the [ACL](#Section_20233ed8a6c64097aafadd545ed24428) on which to search.
* *AceType*: the type of ACE to search.
* *Index*: the index at which to start searching.

**Returns**

* *FoundAce*: The first instance of the specified ACE type to appear at or after the given index.
* *FoundIndex*: The index of *FoundAce* or -1 if no such ACE exists.

1. Initialize NewACE to Empty ACE
2. Initialize FoundIndex to Index
4. FOR each ACE in Acl DO
5. IF ACE.AceType = AceType
6. THEN
7. RETURN ACE, FoundIndex
8. ELSE
9. FoundIndex = FoundIndex +1
10. ENDIF // End If AceType
11. END FOR // End of FOR each Ace in Acl
13. RETURN NULL, -1
14. // END FindAceByType

#### Algorithm for Creating a Security Descriptor

An important element of the overall security model is the manner in which security descriptors are created for new objects. In the trivial case, the creator of a new object simply supplies a new security descriptor for the new object, and the two are associated by the resource manager or server that owns the object. The trivial case is not the common case, however, and the security model has specific behavior involved in deriving the security descriptor for a new object from the security descriptors for existing objects.

The derivation of a new security descriptor in this security model is called inheritance, and refers to the concept that the new security descriptor inherits some or all of its characteristics from the security descriptor of a parent or container object. Individual [ACEs](#Section_d06e5a81176e46c69cf79137aad4455e) can contain indicators that specify whether it can be passed on to child objects, this indicator is called inheritable. Additionally, they can have an indicator as to whether the ACE was derived from a parent during its creation, this indicator is called inherited.

In overview, the process is fairly straightforward. During the creation of a new security descriptor where inheritance is possible, the parent security descriptor is examined. For each ACE in the parent security descriptor, the process checks whether it is marked as inheritable. If so, it is included in the new security descriptor. This is done for both the **DACL** and **SACL** portions of the security descriptor.

The algorithm for computing the system and discretionary [ACL](#Section_20233ed8a6c64097aafadd545ed24428) (**SACL** and **DACL** respectively) in the security descriptor for the new object is governed by the logic that is illustrated in the following figure.

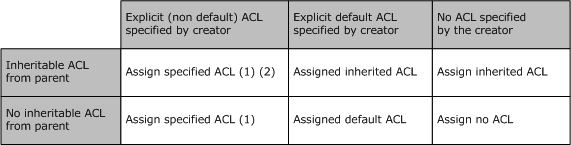


Figure 11: ACL inheritance logic

1. Any ACEs with the INHERITED\_ACE bit set are NOT copied to the assigned security descriptor.
2. If *AutoInheritFlags*, as specified in section [2.5.3.4.1](#Section_98267ad666db4a2c972eefb7d4603da1), is set to automatically inherit ACEs from the parent (DACL\_AUTO\_INHERIT or SACL\_AUTO\_INHERIT), inherited ACEs from the parent are appended after explicit ACEs from the *CreatorDescriptor*. For further details, see the parameter list for CreateSecurityDescriptor (section 2.5.3.4.1).
3. The preceding table describing ACL inheritance logic holds true if the ACL is not protected. If the ACL is protected, all the ACEs from the Explicit ACL are copied into the assigned security descriptor, resetting any ACEs with the INHERITED\_ACE bit set as well. The Inheritable ACL is not considered.

**Note**  An explicitly specified ACL, whether a default ACL or not, can be empty or null.[<93>](#Appendix_A_93" \o "Product behavior note 93)

The remainder of this section documents the details of the algorithm outlined above as a set of nested subprocedures.

##### CreateSecurityDescriptor

This is the top-level routine that assembles the contributions from the parent security descriptor and the creator descriptor and possibly the default **DACL** from the token. This is fairly high-level, and relies primarily upon the subroutine [ComputeACL](#Section_7c59604a945c4f6fa7061cbb80041e83), specified in section 2.5.3.4.2.

**Parameters**

* *ParentDescriptor*: Security descriptor for the parent (container) object of the new object. If the object has no parent, this parameter is null.
* *CreatorDescriptor*: Security descriptor for the new object provided by the creator of the object. Caller can pass null.
* *IsContainerObject*: [BOOLEAN](#Section_51bbfbb108e24c13a95e1eaa7d310670): TRUE when the object is a container; otherwise, FALSE.
* *ObjectTypes*: An array of pointers to [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) structures that identify the object types or classes of the object associated with NewDescriptor (the return value). For Active Directory objects, this array contains pointers to the class GUIDs of the object's structural class and all attached auxiliary classes. If the object for which this descriptor is being created does not have a GUID, this field MUST be set to null.
* *AutoInheritFlags*: A set of bit flags that control how [access control entries (ACEs)](#Section_d06e5a81176e46c69cf79137aad4455e) are inherited from *ParentDescriptor*. This parameter can be a combination of the following values:
  + DACL\_AUTO\_INHERIT: If set, inheritable ACEs from the parent security descriptor **DACL** are merged with the explicit ACEs in the *CreatorDescriptor*.
  + SACL\_AUTO\_INHERIT: If set, inheritable ACEs from the parent security descriptor **SACL** are merged with the explicit ACEs in the *CreatorDescriptor*.
  + DEFAULT\_DESCRIPTOR\_FOR\_OBJECT: Selects the *CreatorDescriptor* as the default security descriptor provided that no object type specific ACEs are inherited from the parent. If such ACEs do get inherited, *CreatorDescriptor* is ignored.
  + DEFAULT\_OWNER\_FROM\_PARENT: Relevant only when the owner field is not specified in *CreatorDescriptor*. If this flag is set, the owner field in *NewDescriptor* is set to the owner of *ParentDescriptor*. If not set, the owner from the token is selected.
  + DEFAULT\_GROUP\_FROM\_PARENT: Relevant only when the primary group field is not specified in *CreatorDescriptor*. If this flag is set, the primary group of *NewDescriptor* is set to the primary group of *ParentDescriptor*. If not set, the default group from the token is selected.
* *Token*: Authorization context supplied that contains the ownership information as well as the default **DACL** if the default **DACL** is necessary.
* *GenericMapping*: Mapping of generic permissions to resource manager-specific permissions supplied by the caller.

**Returns**

* *NewDescriptor*: Output security descriptor for the object computed by the algorithm.

1. // Step 1:Compute the Owner field. If there is no specified owner,
2. // then determine an appropriate owner.
3. IF CreatorDescriptor.Owner is NULL THEN
4. IF AutoInheritFlags contains DEFAULT\_OWNER\_FROM\_PARENT THEN
5. Set NewDescriptor.Owner to ParentDescriptor.Owner
6. ELSE
7. Set NewDescriptor.Owner to Token.SIDs[Token.OwnerIndex]
8. ENDIF
9. ELSE
10. Set NewDescriptor.Owner to CreatorDescriptor.Owner
11. ENDIF
12. // Step 2:Compute the Group field. If there is no specified groups,
13. // then determine the appropriate group.
14. IF CreatorDescriptor.Group is NULL THEN
15. IF AutoInheritFlags contains DEFAULT\_GROUP\_FROM\_PARENT THEN
16. Set NewDescriptor.Group to ParentDescriptor.Group
17. ELSE
18. Set NewDescriptor.Group to Token.SIDs[Token.PrimaryGroup]
19. ENDIF
20. ELSE
21. Set NewDescriptor.Group to CreatorDescriptor.Group
22. ENDIF
23. // Step 3:Compute the DACL
24. CALL ComputeACL WITH
25. ComputeType set to COMPUTE\_DACL,
26. ParentACL set to ParentDescriptor.DACL,
27. AuthoInheritFlags set to AutoInheritFlags,
28. ParentControl set to ParentDescriptor.Control,
29. CreatorACL set to CreatorDescriptor.DACL,
30. CreatorControl set to CreatorDescriptor.Control
31. IsContainerObject set to IsContainerObject,
32. ObjectTypes set to ObjectTypes,
33. GenericMapping set to GenericMapping,
34. Owner set to NewDescriptor.Owner,
35. Group set to NewDescriptor.Group,
36. Token set to Token
37. RETURNING NewDACL, NewControl
38. Set NewDescriptor.DACL to NewDACL
39. Set NewDescriptor.Control to NewControl
40. // Step 4:Compute the SACL
41. CALL ComputeACL WITH
42. ComputeType set to COMPUTE\_SACL,
43. ParentACL set to ParentDescriptor.SACL,
44. AutoInheritFlags set to AutoInheritFlags,
45. ParentControl set to ParentDescriptor.Control,
46. CreatorACL set to CreatorDescriptor.SACL,
47. CreatorControl set to CreatorDescriptor.Control,
48. IsContainerObject set to IsContainerObject,
49. ObjectTypes set to ObjectTypes,
50. GenericMapping set to GenericMapping,
51. Owner set to NewDescriptor.Owner,
52. Group set to NewDescriptor.Group,
53. Token set to Token
54. RETURNING NewSACL, NewControl
55. Set NewDescriptor.SACL to NewSACL
56. Set NewDescriptor.Control to (NewDescriptor.Control OR NewControl)
57. RETURN NewDescriptor
58. // END CreateSecurityDescriptor

##### ComputeACL

The ComputeACL subroutine determines the new [ACL](#Section_20233ed8a6c64097aafadd545ed24428) based on supplied Parent ACL, Creator ACL, and possibly the Token's DefaultDACL, depending on the supplied parameters and policy. This function is generally applicable to both the **DACL** and **SACL** portions of the security descriptor, although there are some specific behaviors that differ between the two types of **DACL**, so care has to be taken during implementation to honor the ComputeType parameter.

**Parameters**

* *ComputeType*: Enumeration of COMPUTE\_DACL and COMPUTE\_SACL.
* *ParentACL*: ACL from the parent security descriptor.
* *AutoInheritFlags*: as specified in section [2.5.3.4.1](#Section_98267ad666db4a2c972eefb7d4603da1). Note that it is possible to have the DACL\_AUTO\_INHERIT flag set when *ComputeType* is set to COMPUTE\_SACL (or vice-versa).
* *ParentControl*: Control flags from the parent security descriptor.
* *CreatorACL*: ACL supplied in the security descriptor by the creator.
* *CreatorControl*: Control flags supplied in the security descriptor by the creator.
* *IsContainerObject*: TRUE if the object is a container; otherwise, FALSE.
* *ObjectTypes*: Array of [**GUIDs**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) for the object type being created.
* *GenericMapping*: Mapping of generic permissions to resource manager-specific permissions supplied by the caller.
* *Owner*: Owner to use in substituting the *CreatorOwner* SID.
* *Group*: Group to use in substituting the *CreatorGroup* SID.
* *Token*: Token for default values.

**Returns**

* Computed ACL
* ComputedControl

1. // The details of the algorithm to merge the parent ACL and the supplied ACL.
2. // The Control flags computed are slightly different based on whether it is the
3. // ACL in the DACL or the SACL field of the descriptor.
4. // The caller specifies whether it is a DACL or a SACL using the parameter,
5. // ComputeType.
6. Set ComputedACL to NULL
7. Set ComputedControl to NULL
8. CALL ContainsInheritableACEs WITH ParentACL RETURNING ParentHasInheritableACEs
9. IF ParentHasInheritableACEs = TRUE THEN
10. // The Parent ACL has inheritable ACEs. The Parent ACL should be used if no Creator
11. // ACL is supplied, or if the Creator ACL was supplied AND it is a default ACL based
12. // on object type information
13. IF(CreatorACL is not present) OR
14. ((CreatorACL is present) AND
15. (AutoInheritFlags contains DEFAULT\_DESCRIPTOR\_FOR\_OBJECT))
16. THEN
17. // Use only the inherited ACEs from the parent. First compute the ACL from the
18. // parent ACL, then clean it up by resolving the generic mappings etc.
19. CALL ComputeInheritedACLFromParent WITH
20. ACL set to ParentACL,
21. IsContainerObject set to IsContainerObject,
22. ObjectTypes set to ObjectTypes
23. RETURNING NextACL
24. CALL PostProcessACL WITH
25. ACL set to NextACL,
26. CopyFilter set to CopyInheritedAces,
27. Owner set to Owner,
28. Group set to Group,
29. GenericMapping set to GenericMapping
30. RETURNING FinalACL
31. Set ComputedACL to FinalACL
32. RETURN
33. ENDIF
34. IF ((CreatorACL is present) AND
35. (AutoInheritFlags does not contain DEFAULT\_DESCRIPTOR\_FOR\_OBJECT))
36. THEN
37. // Since a creator ACL is present, and we're not defaulting the
38. // descriptor, determine which ACEs are inherited and compute the new ACL
39. CALL PreProcessACLFromCreator WITH
40. ACL set to CreatorACL
41. RETURNING PreACL
42. CALL ComputeInheritedACLFromCreator WITH
43. ACL set to PreACL,
44. IsContainerObject set to IsContainerObject,
45. ObjectTypes set to ObjectTypes
46. RETURNING TmpACL
47. // Special handling for DACL types of ACLs
48. IF (ComputeType = DACL\_COMPUTE) THEN
50. // DACL-specific operations
51. IF (CreatorControl does not have DACL\_PROTECTED flag set) AND
52. (AutoInheritFlags contains DACL\_AUTO\_INHERIT)
53. THEN
54. // We're not working from a protected DACL, and we're supposed to
55. // allow automatic inheritance. Compute the inherited ACEs from
56. // Parent ACL this time, and append that to the ACL that we're building
57. CALL ComputeInheritedACLFromParent WITH
58. ACL set to ParentACL,
59. IsContainerObject set to IsContainerObject,
60. ObjectTypes set to ObjectTypes
61. RETURNING InheritedParentACL
62. Append InheritedParentACL.ACEs to TmpACL.ACE
63. Set DACL\_AUTO\_INHERITED flag in ComputedControl
64. ENDIF
65. ENDIF // DACL-Specific behavior
66. IF (ComputeType = SACL\_COMPUTE) THEN
67. // Similar to the above, perform SACL-specific operations
68. IF (CreatorControl does not have SACL\_PROTECTED flag set) AND
69. (AutoInheritFlags contains SACL\_AUTO\_INHERIT flag)
70. THEN
71. // We're not working from a protected SACL, and we're supposed to
72. // allow automatic inheritance. Compute the inherited ACEs from
73. // Parent ACL this time, and append that to the ACL that we're building
74. CALL ComputeInheritedACLFromParent WITH
75. ACL set to ParentACL,
76. IsContainerObject set to IsContainerObject,
77. ObjectTypes set to ObjectTypes
78. RETURNING InheritedParentACL
79. Append InheritedParentACL.ACEs to TmpACL.ACE
80. Set SACL\_AUTO\_INHERITED flag in ComputedControl
81. ENDIF
82. ENDIF // SACL-Specific behavior
84. CALL PostProcessACL WITH
85. ACL set to TmpACL,
86. CopyFilter set to CopyInheritedAces,
87. Owner set to Owner,
88. Group set to Group,
89. GenericMapping set to GenericMapping
90. RETURNING ProcessedACL
91. Set ComputedACL to ProcessedACL
92. RETURN
93. ENDIF // CreatorACL is present
94. ELSE // ParentACL does not contain inheritable ACEs
95. IF CreatorACL = NULL THEN
96. // No ACL supplied for the object
97. IF (ComputeType = DACL\_COMPUTE) THEN
98. Set TmpACL to Token.DefaultDACL
99. ELSE
100. // No default for SACL; left as NULL
101. ENDIF
102. ELSE
103. // Explicit ACL was supplied for the object - either default or not.
104. // In either case, use it for the object, since there are no inherited ACEs.
105. CALL PreProcessACLFromCreator WITH CreatorACL
106. RETURNING TmpACL
107. ENDIF
108. CALL PostProcessACL WITH
109. ACL set to TmpACL,
110. CopyFilter set to CopyAllAces,
111. Owner set to Owner,
112. Group set to Group,
113. GenericMapping set to GenericMapping
114. RETURNING ProcessedACL
115. Set ComputedACL to ProcessedACL
116. ENDIF
117. // END ComputeACL

##### ContainsInheritableACEs

**Parameters**

* *ACL*

**Returns**

* TRUE or FALSE

1. // Computes whether the ACL parameter contains any ACEs that are inheritable
2. // by a child
3. // True: if it contains any inheritable ACEs
4. // False: otherwise
5. FOR each ACE in ACL DO
6. IF(ACE.AceFlags contains CONTAINER\_INHERIT\_ACE) OR
7. (ACE.AceFlags contains OBJECT\_INHERIT\_ACE)
8. THEN
9. RETURN TRUE
10. ENDIF
11. END FOR
12. RETURN FALSE
13. // END ContainsInheritableACEs

##### ComputeInheritedACLfromParent

This subroutine copies the [ACEs](#Section_d06e5a81176e46c69cf79137aad4455e) from an [ACL](#Section_20233ed8a6c64097aafadd545ed24428) that are marked as inheritable. These ACEs are assembled into a new ACL that is returned.

**Parameters**

* *ACL*: An ACL that contains the parent's ACEs from which to compute the inherited ACL.
* *IsContainerObject*: TRUE if the object is a container; otherwise, FALSE.
* *ObjectTypes*: An array of [**GUIDs**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) for the object type being created.

**Returns**

* The computed ACL that also includes the inherited ACEs.

1. // Computes the inheritable and inherited ACEs to propagate to the new object
2. // from the inheritable ACEs in the parent container object
3. Initialize ExplicitACL to Empty ACL
4. FOR each ACE in ACL DO
5. IF ACE.AceFlags contains INHERIT\_ONLY\_ACE
6. THEN
7. CONTINUE
8. ENDIF
9. IF(((ACE.AceFlags contains CONTAINER\_INHERIT\_ACE) AND
10. (IsContainerObject = TRUE))OR
11. ((ACE.AceFlags contains OBJECT\_INHERIT\_ACE) AND
12. (IsContainerObject = FALSE)))
13. THEN
14. CASE ACE.Type OF
15. ACCESS\_ALLOWED\_ACE\_TYPE:
16. ACCESS\_DENIED\_ACE\_TYPE:
17. Create empty NewACE
18. Copy ACE to NewACE
19. Clear NewACE.AceFlags –- no flags set
20. NewACE.AceFlags = INHERITED\_ACE
21. Append NewACE to ExplicitACL
22. ACCESS\_ALLOWED\_OBJECT\_ACE\_TYPE:
23. ACCESS\_DENIED\_OBJECT\_ACE\_TYPE:
24. IF (ObjectTypes contains ACE.ObjectGUID) THEN
25. Create empty NewACE
26. Copy ACE to NewACE
27. Clear NewACE.AceFlags –- no flags set
28. NewACE.AceFlags = INHERITED\_ACE
29. Append NewACE to ExplicitACL
30. ENDIF
31. ENDCASE
32. ENDIF
33. END FOR
34. Initialize InheritableACL to Empty ACL
35. IF (IsContainerObject = TRUE) THEN
36. FOR each ACE in ACL DO
37. IF ACE.AceFlags does not contain NO\_PROPAGATE\_INHERIT\_ACE THEN
38. IF((ACE.AceFlags contains CONTAINER\_INHERIT\_ACE) OR
39. (ACE.AceFlags contains OBJECT\_INHERIT\_ACE))
40. THEN
41. Set NewACE to ACE
42. Add INHERITED\_ACE to NewACE.AceFlags
43. Add INHERIT\_ONLY\_ACE to NewACE.AceFlags
44. Append NewACE to InheritableACL
45. ENDIF
46. ENDIF
47. END FOR
48. ENDIF
49. RETURN concatenation of ExplicitACL and InheritableACL
50. // END ComputeInheritedACLFromParent

There are seven flags that can appear in an ACE. Of the seven flags, the following pertain to inheritance.

* **CI**: CONTAINER\_INHERIT\_ACE
* **OI**: OBJECT\_INHERIT\_ACE
* **NP**: NO\_PROPAGATE\_INHERIT\_ACE
* **IO**: INHERIT\_ONLY\_ACE
* **ID**: INHERITED\_ACE

**IO** and **ID** do not play a part when it comes to making decisions about inheritance. The **ID** flag is added to any ACE that is inherited to indicate that it was inherited. The **IO** flag is used to indicate that an ACE is not effective for the child that inherits the ACE. An ACE that has the **IO** flag can be inherited, but the decision is based on other flags, if present.

The following table summarizes the inherited ACE flags for the child container and child leaf (non-container) object based on the parent ACE flags.

| Parent ACE flags | Child container object | Child leaf object |
| --- | --- | --- |
| No Flags, IO | No Inheritance | No Inheritance |
| OI | IO,OI | Inherited, No flags |
| OI,NP | No Inheritance | Inherited, No flags |
| CI | CI | No Inheritance |
| CI,NP | Inherited, No flags | No Inheritance |
| CI,OI | IO,CI,OI | Inherited, No flags |
| CI,OI,NP | Inherited, No flags | Inherited, No flags |

For the cases in which a container inherits an ACE that is both effective on the container and inheritable by its descendents, the container can inherit two ACEs. This occurs when an inheritable ACE contains generic  information. The container inherits an ACE with an additional **IO** flag with generic information and an effective-only ACE in which the generic information has been mapped.

##### ComputeInheritedACLfromCreator

**Parameters**

* *ACL*: An [ACL](#Section_20233ed8a6c64097aafadd545ed24428) supplied in the security descriptor by the caller.
* *IsContainerObject*: TRUE if the object is a container; otherwise, FALSE.
* *ObjectTypes*: An array of [**GUIDs**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) for the object type being created.

**Returns**

* The computed ACL that also includes the inherited ACEs.

1. // Computes the inheritable and inherited ACEs to propagate to the new object
2. // from any inheritable ACEs in the ACL supplied by the caller
3. Initialize ExplicitACL to Empty ACL
4. FOR each ACE in ACL DO
5. IF((ACE.AceFlags contains CONTAINER\_INHERIT\_ACE) AND
6. (IsContainerObject = TRUE))OR
7. ((ACE.AceFlags contains OBJECT\_INHERIT\_ACE) AND
8. (IsContainerObject = FALSE))
9. THEN
10. CASE ACE.Type OF
11. ALLOW:
12. DENY:
13. Set NewACE to ACE
14. Set NewACE.AceFlags to NULL
15. Append NewACE to ExplicitACL
16. OBJECT\_ALLOW
17. OBJECT\_DENY:
18. IF (ObjectTypes contains ACE.ObjectGUID) THEN
19. Set NewACE to ACE
20. Set NewACE.AceFlags to NULL
21. Append NewACE to ExplicitACL
22. ENDIF
23. ENDCASE
24. ENDIF
25. END FOR
26. Initialize InheritableACL to Empty ACL
27. IF (IsContainerObject = TRUE) THEN
28. FOR each ACE in ACL DO
29. IF((ACE.AceFlags contains CONTAINER\_INHERIT\_ACE) OR
30. (ACE.AceFlags contains OBJECT\_INHERIT\_ACE))
31. THEN
32. Set NewACE to ACE
33. Add INHERIT\_ONLY\_ACE to NewACE.AceFlags
34. Append NewACE to InheritableACL
35. ENDIF
36. END FOR
37. ENDIF
38. RETURN concatenation of ExplicitACL and InheritableACL
39. // END ComputeInheritedACLFromCreator

##### PreProcessACLfromCreator

This subroutine processes an input [ACL](#Section_20233ed8a6c64097aafadd545ed24428), removing all [ACEs](#Section_d06e5a81176e46c69cf79137aad4455e) that were inherited previously, yielding an ACL with only explicit ACEs.

**Parameters**

* *ACL*: ACL to preprocess.

**Returns**

* Processed ACL.

1. Initialize NewACL to Empty ACL
2. FOR each ACE in ACL DO
3. IF ACE.AceFlags does not contain INHERITED\_ACE THEN
4. Append ACE to NewACL
5. ENDIF
6. END FOR
7. RETURN NewACL
8. // END PreProcessACLFromCreator

##### PostProcessACL

The purpose of this subroutine is to process the [ACL](#Section_20233ed8a6c64097aafadd545ed24428) and make it concrete by replacing certain macro [SIDs](#Section_78eb90131c3a4970ad1f2b1dad588a25) with the actual SIDs for the principals involved, and to translate from generic access bit flags to the actual object-specific access flags. The caller specifies a filter to apply, namely whether only inherited [ACEs](#Section_d06e5a81176e46c69cf79137aad4455e), only explicit ACEs, or all ACEs will be copied.

**Parameters**

* *ACL*: ACL on which to substitute SIDs.
* CopyFilter: Enumeration of the following filters for post-processing the ACL: **CopyAllAces**, **CopyInheritedAces**, **CopyExplicitAces**.
* *Owner*: Owner to use in substituting the *CreatorOwner* SID.
* *Group*: Group to use in substituting the *CreatorGroup* SID.
* *GenericMapping*: Mapping of generic permissions to resource manager-specific permissions supplied by the caller.

**Returns**

* The computed ACL with the SID substitutions performed.

1. // Substitute CreatorOwner and CreatorGroup SIDs and do GenericMapping in ACL
2. Initialize NewACL to Empty ACL
3. FOR each ACE in ACL DO
4. // Determine if this ACE passes the filter to be copied to the new ACL
5. SET CopyThisAce = FALSE
6. CASE CopyFilter OF
8. CopyAllAces:
9. BEGIN
10. SET CopyThisAce = TRUE
11. END
12. CopyInheritedAces:
13. BEGIN
14. IF (ACE.AceFlags contains INHERITED\_ACE) THEN
15. SET CopyThisAce = TRUE
16. ENDIF
17. END
18. CopyExplicitAces:
19. BEGIN
20. IF (ACE.AceFlags does not contain INHERITED\_ACE) THEN
21. SET CopyThisAce = TRUE
22. ENDIF
23. END
24. ENDCASE
25. Set NewACE to ACE
26. IF (CopyThisAce) THEN
27. CASE ACE.Sid OF
28. CREATOR\_OWNER:
29. NewACE.Sid = Owner
30. CREATOR\_GROUP:
31. NewACE.Sid = Group
32. ENDCASE
33. IF (ACE.Mask contains GENERIC\_READ) THEN
34. Add GenericMapping.GenericRead to NewACE.Mask
35. ENDIF
36. IF (ACE.Mask contains GENERIC\_WRITE) THEN
37. Add GenericMapping.GenericWrite to NewACE.Mask
38. ENDIF
39. IF (ACE.Mask contains GENERIC\_EXECUTE) THEN
40. Add GenericMapping.GenericExecute to NewACE.Mask
41. ENDIF
42. Append NewACE to NewACL
43. ENDIF
44. END FOR
45. RETURN NewACL
46. // END PostProcessACL

## ServerGetInfo Abstract Interface

The ServerGetInfo abstract interface retrieves current configuration information for the local machine.

1. DWORD ServerGetInfo(
2. [in] DWORD level,
3. [out] LPBYTE\* bufptr
4. );

**level**: Specifies the information level of the data. This parameter can be one of the following values.

| Value | Meaning |
| --- | --- |
| 100 | Return the machine name and platform information. The *bufptr* parameter points to a [SERVER\_INFO\_100](#Section_007c654b7d7849d49f4d0da7c1889727) structure. |
| 101 | Return the machine name, type, and associated software. The *bufptr* parameter points to a [SERVER\_INFO\_101](#Section_39c502dd022b4a68936789fd76a23bc3) structure. |

**bufptr**: Pointer to the buffer that receives the data. The format of this data depends on the value of the level parameter.

**Note**  When the 101 information level is requested, the machine is considered to be a domain controller (SV\_TYPE\_DOMAIN\_CTRL or SV\_TYPE\_DOMAIN\_BAKCTRL) when it supports the protocols required by the Active Directory Domain Service system (either with or without Web Services) as described in [[MS-ADOD]](%5bMS-ADOD%5d.pdf#Section_5ff67bf4c14548cb89cd4f5482d94664) section 2.8. Once it is established that the machine is a domain controller, it is considered to be a primary domain controller (SV\_TYPE\_DOMAIN\_CTRL) if it is currently hosting the PdcEmulationMasterRole FSMO role (as specified in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.1.11); otherwise it is considered to be a backup domain controller (SV\_TYPE\_DOMAIN\_BAKCTRL). The machine determines whether it is hosting the PdcEmulationMasterRole by invoking the **IsEffectiveRoleOwner** function with the *roleObject* parameter set to RoleObject(Default NC, PdcEmulationMasterRole) (see [MS-ADTS] section 3.1.1.5.1.8). When the 101 information level is requested, and the machine is not considered to be a domain controller as specified above, then it is considered to be a workstation (SV\_TYPE\_WORKSTATION). Additional SV\_TYPE\_\* values can be returned as appropriate.

**Return Values**: If the function succeeds, the return value is NERR\_Success.

If the function fails, the return value can be one of the following error codes:

| Return value/code | Description |
| --- | --- |
| 0x00000005  ERROR\_ACCESS\_DENIED | The user does not have access to the requested information. |
| 0x0000007C  ERROR\_INVALID\_LEVEL | The value specified for the level parameter is invalid. |
| 0x00000057  ERROR\_INVALID\_PARAMETER | The specified parameter is invalid. |
| 0x00000008  ERROR\_NOT\_ENOUGH\_MEMORY | Sufficient memory is not available. |

## Impersonation Abstract Interfaces

### StartImpersonation

The StartImpersonation abstract interface causes the underlying security infrastructure for a server role to use the supplied **ImpersonationAccessToken** for access checks on secured objects until either the [EndImpersonation](#Section_2eaaa78a77f748d58ef3882809c0bc83) abstract interface is called or a further call to StartImpersonation is called with a new ImpersonationAccessToken. When the EndImpersonation abstract interface is called, the security infrastructure reverts to using the primary token (see [[MSDN-ACCTOKENS]](https://go.microsoft.com/fwlink/?LinkId=89949)). The invocation of the StartImpersonation interface is the equivalent to supplying the *ImpersonationAccessToken* as the *Token* parameter to the Access Check Algorithm defined in section [2.5.3.2](#Section_4f1bbcbb814a4c70a11e2a5b8779a6f9).

See also [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15), Abstract Interface RpcImpersonateClient (section 3.3.3.4.3.2) and Abstract Interface RpcRevertToSelf (section 3.3.3.4.3.3), for RPC-specific versions of the impersonation abstraction, and [Tanenbaum] section 11.8, Security in Windows 2000.

1. void StartImpersonation(
2. [in] Token ImpersonationAccessToken
3. );

**ImpersonationAccessToken**: An authorization context token as specified in section [2.5.2](#Section_efc83c3252754dffa3e2973c9624711b).

This method has no return values.

### EndImpersonation

The EndImpersonation abstract interface causes the underlying security infrastructure for a server role to revert to using the primary access token (see [[MSDN-ACCTOKENS]](https://go.microsoft.com/fwlink/?LinkId=89949)) for access checks on secured objects.

1. void EndImpersonation(
2. void
3. );

This method has no return values.

### GetAccessToken

The GetAccessToken abstract interface causes the underlying security infrastructure for the server role to return the [Token/Authorization Context](#Section_efc83c3252754dffa3e2973c9624711b), as specified in section 2.5.2, of the current execution context.

If no prior call has been made to [StartImpersonation()](#Section_d487a5cf2c774e66a100ac90cbaca94d) in the current execution context, the call returns the *primary* access token (see [[MSDN-ACCTOKENS]](https://go.microsoft.com/fwlink/?LinkId=89949)) of the security principal that is associated with the current execution context.

If a call to StartImpersonation() has been performed without a subsequent call to [EndImpersonation()](#Section_2eaaa78a77f748d58ef3882809c0bc83), the call returns the *impersonation* access token as the *Token* parameter to the Access Check Algorithm defined in section [2.5.3.2](#Section_4f1bbcbb814a4c70a11e2a5b8779a6f9).

1. Token GetAccessToken();

**Return Values**: This method returns a Token/Authorization Context, as specified in section 2.5.2, of the current execution context.

# Structure Examples

There are no structure examples.

# Security Considerations

There are no security considerations.

# Appendix A: Full MS-DTYP IDL

For ease of implementation and to allow re-use of the common data types and structure in other protocols, a full [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) is provided.

1. typedef unsigned short wchar\_t;
2. typedef void\* ADCONNECTION\_HANDLE;
3. typedef int BOOL, \*PBOOL, \*LPBOOL;
4. typedef unsigned char BYTE, \*PBYTE, \*LPBYTE;
5. typedef BYTE BOOLEAN, \*PBOOLEAN;
6. typedef wchar\_t WCHAR, \*PWCHAR;
7. typedef WCHAR\* BSTR;
8. typedef char CHAR, \*PCHAR;
9. typedef double DOUBLE;
10. typedef unsigned long DWORD, \*PDWORD, \*LPDWORD;
11. typedef unsigned int DWORD32;
12. typedef unsigned \_\_int64 DWORD64, \*PDWORD64;
13. typedef unsigned \_\_int64 ULONGLONG;
14. typedef ULONGLONG DWORDLONG, \*PDWORDLONG;
15. typedef unsigned long error\_status\_t;
16. typedef float FLOAT;
17. typedef unsigned char UCHAR, \*PUCHAR;
18. typedef short SHORT;
19. typedef void\* HANDLE;
20. typedef DWORD HCALL;
21. typedef int INT, \*LPINT;
22. typedef signed char INT8;
23. typedef signed short INT16;
24. typedef signed int INT32;
25. typedef signed \_\_int64 INT64;
26. typedef void\* LDAP\_UDP\_HANDLE;
27. typedef const wchar\_t\* LMCSTR;
28. typedef WCHAR\* LMSTR;
29. typedef long LONG, \*PLONG, \*LPLONG;
30. typedef signed \_\_int64 LONGLONG;
31. typedef LONG HRESULT;
32. typedef \_\_int3264 LONG\_PTR;
33. typedef unsigned \_\_int3264 ULONG\_PTR;
34. typedef signed int LONG32;
35. typedef signed \_\_int64 LONG64, \*PLONG64;
36. typedef const char\* LPCSTR;
37. typedef const void\* LPCVOID;
38. typedef const wchar\_t\* LPCWSTR;
39. typedef char\* PSTR, \*LPSTR;
40. typedef wchar\_t\* LPWSTR, \*PWSTR;
41. typedef DWORD NET\_API\_STATUS;
42. typedef long NTSTATUS;
43. typedef [context\_handle] void\* PCONTEXT\_HANDLE;
44. typedef [ref] PCONTEXT\_HANDLE\* PPCONTEXT\_HANDLE;
46. typedef unsigned \_\_int64 QWORD;
47. typedef void\* RPC\_BINDING\_HANDLE;
48. typedef UCHAR\* STRING;
49. typedef unsigned int UINT;
50. typedef unsigned char UINT8;
51. typedef unsigned short UINT16;
52. typedef unsigned int UINT32;
53. typedef unsigned \_\_int64 UINT64;
54. typedef unsigned long ULONG, \*PULONG;
55. typedef ULONG\_PTR DWORD\_PTR;
56. typedef ULONG\_PTR SIZE\_T;
57. typedef unsigned int ULONG32;
58. typedef unsigned \_\_int64 ULONG64;
59. typedef wchar\_t UNICODE;
60. typedef unsigned short USHORT;
61. typedef void VOID, \*PVOID, \*LPVOID;
62. typedef unsigned short WORD, \*PWORD, \*LPWORD;
63. typedef struct \_FILETIME {
64. DWORD dwLowDateTime;
65. DWORD dwHighDateTime;
66. } FILETIME,
67. \*PFILETIME,
68. \*LPFILETIME;
69. typedef struct \_GUID {
70. unsigned long Data1;
71. unsigned short Data2;
72. unsigned short Data3;
73. byte Data4[8];
74. } GUID,
75. UUID,
76. \*PGUID;
77. typedef struct \_LARGE\_INTEGER {
78. signed \_\_int64 QuadPart;
79. } LARGE\_INTEGER, \*PLARGE\_INTEGER;
80. typedef struct \_EVENT\_DESCRIPTOR {
81. USHORT Id;
82. UCHAR Version;
83. UCHAR Channel;
84. UCHAR Level;
85. UCHAR Opcode;
86. USHORT Task;
87. ULONGLONG Keyword;
88. } EVENT\_DESCRIPTOR,
89. \*PEVENT\_DESCRIPTOR,
90. \*PCEVENT\_DESCRIPTOR;
91. typedef struct \_EVENT\_HEADER {
92. USHORT Size;
93. USHORT HeaderType;
94. USHORT Flags;
95. USHORT EventProperty;
96. ULONG ThreadId;
97. ULONG ProcessId;
98. LARGE\_INTEGER TimeStamp;
99. GUID ProviderId;
100. EVENT\_DESCRIPTOR EventDescriptor;
101. union {
102. struct {
103. ULONG KernelTime;
104. ULONG UserTime;
105. };
106. ULONG64 ProcessorTime;
107. };
108. GUID ActivityId;
109. } EVENT\_HEADER,
110. \*PEVENT\_HEADER;
111. typedef DWORD LCID;
112. typedef struct \_LUID {
113. DWORD LowPart;
114. LONG HighPart;
115. } LUID,
116. \*PLUID;
117. typedef struct \_MULTI\_SZ {
118. wchar\_t\* Value;
119. DWORD nChar;
120. } MULTI\_SZ;
121. typedef struct \_RPC\_UNICODE\_STRING {
122. unsigned short Length;
123. unsigned short MaximumLength;
124. [size\_is(MaximumLength/2), length\_is(Length/2)]
125. WCHAR\* Buffer;
126. } RPC\_UNICODE\_STRING,
127. \*PRPC\_UNICODE\_STRING;
128. typedef struct \_SERVER\_INFO\_100 {
129. DWORD sv100\_platform\_id;
130. [string] wchar\_t\* sv100\_name;
131. } SERVER\_INFO\_100,
132. \*PSERVER\_INFO\_100,
133. \*LPSERVER\_INFO\_100;
134. typedef struct \_SERVER\_INFO\_101 {
135. DWORD sv101\_platform\_id;
136. [string] wchar\_t\* sv101\_name;
137. DWORD sv101\_version\_major;
138. DWORD sv101\_version\_minor;
139. DWORD sv101\_version\_type;
140. [string] wchar\_t\* sv101\_comment;
141. } SERVER\_INFO\_101,
142. \*PSERVER\_INFO\_101,
143. \*LPSERVER\_INFO\_101;
144. typedef struct \_SYSTEMTIME {
145. WORD wYear;
146. WORD wMonth;
147. WORD wDayOfWeek;
148. WORD wDay;
149. WORD wHour;
150. WORD wMinute;
151. WORD wSecond;
152. WORD wMilliseconds;
153. } SYSTEMTIME,
154. \*PSYSTEMTIME;
155. typedef struct \_UINT128 {
156. UINT64 lower;
157. UINT64 upper;
158. } UINT128,
159. \*PUINT128;
160. typedef struct \_ULARGE\_INTEGER {
161. unsigned \_\_int64 QuadPart;
162. } ULARGE\_INTEGER, \*PULARGE\_INTEGER;
163. typedef struct \_RPC\_SID\_IDENTIFIER\_AUTHORITY {
164. byte Value[6];
165. } RPC\_SID\_IDENTIFIER\_AUTHORITY;
166. typedef DWORD ACCESS\_MASK;
167. typedef ACCESS\_MASK \*PACCESS\_MASK;
168. typedef struct \_OBJECT\_TYPE\_LIST {
169. WORD Level;
170. ACCESS\_MASK Remaining;
171. GUID\* ObjectType;
172. } OBJECT\_TYPE\_LIST,
173. \*POBJECT\_TYPE\_LIST;
174. typedef struct \_ACE\_HEADER {
175. UCHAR AceType;
176. UCHAR AceFlags;
177. USHORT AceSize;
178. } ACE\_HEADER,
179. \*PACE\_HEADER;
180. typedef struct \_SYSTEM\_MANDATORY\_LABEL\_ACE {
181. ACE\_HEADER Header;
182. ACCESS\_MASK Mask;
183. DWORD SidStart;
184. } SYSTEM\_MANDATORY\_LABEL\_ACE,
185. \*PSYSTEM\_MANDATORY\_LABEL\_ACE;
186. typedef struct \_TOKEN\_MANDATORY\_POLICY {
187. DWORD Policy;
188. } TOKEN\_MANDATORY\_POLICY,
189. \*PTOKEN\_MANDATORY\_POLICY;
190. typedef struct \_MANDATORY\_INFORMATION {
191. ACCESS\_MASK AllowedAccess;
192. BOOLEAN WriteAllowed;
193. BOOLEAN ReadAllowed;
194. BOOLEAN ExecuteAllowed;
195. TOKEN\_MANDATORY\_POLICY MandatoryPolicy;
196. } MANDATORY\_INFORMATION,
197. \*PMANDATORY\_INFORMATION;
198. typedef struct \_CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE {
199. DWORD Length;
200. BYTE OctetString[];
201. } CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE,
202. \*PCLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE;
203. typedef struct \_CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 {
204. DWORD Name;
205. WORD ValueType;
206. WORD Reserved;
207. DWORD Flags;
208. DWORD ValueCount;
209. union {
210. PLONG64 pInt64[];
211. PDWORD64 pUint64[];
212. PWSTR ppString[];
213. PCLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE pOctetString[];
214. } Values;
215. } CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1,
216. \*PCLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1;
217. typedef DWORD SECURITY\_INFORMATION, \*PSECURITY\_INFORMATION;
218. typedef struct \_RPC\_SID {
219. unsigned char Revision;
220. unsigned char SubAuthorityCount;
221. RPC\_SID\_IDENTIFIER\_AUTHORITY IdentifierAuthority;
222. [size\_is(SubAuthorityCount)] unsigned long SubAuthority[];
223. } RPC\_SID,
224. \*PRPC\_SID,
225. \*PSID;
226. typedef struct \_ACL {
227. unsigned char AclRevision;
228. unsigned char Sbz1;
229. unsigned short AclSize;
230. unsigned short AceCount;
231. unsigned short Sbz2;
232. } ACL,
233. \*PACL;
234. typedef struct \_SECURITY\_DESCRIPTOR {
235. UCHAR Revision;
236. UCHAR Sbz1;
237. USHORT Control;
238. PSID Owner;
239. PSID Group;
240. PACL Sacl;
241. PACL Dacl;
242. } SECURITY\_DESCRIPTOR,
243. \*PSECURITY\_DESCRIPTOR;

# Appendix B: Product Behavior

* Windows NT operating system
* Windows 2000 operating system
* Windows XP operating system
* Windows Server 2003 operating system
* Windows Vista operating system
* Windows Server 2008 operating system
* Windows 7 operating system
* Windows Server 2008 R2 operating system
* Windows 8 operating system
* Windows Server 2012 operating system
* Windows 8.1 operating system
* Windows Server 2012 R2 operating system
* Windows 10 operating system
* Windows Server 2016 operating system
* Windows Server operating system

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

[<1> Section 2.1](#Appendix_A_Target_1): Windows is implemented on little-endian systems.

[<2> Section 2.3.8](#Appendix_A_Target_2): Windows implementations access the Value field with non-standard string functions to add or extract strings from the buffer. If standard C conventions were followed, the Value datatype would nominally be wchar\_t\*\*.

[<3> Section 2.4.1](#Appendix_A_Target_3): Only Windows Server 2012 and Windows Server 2012 R2 acting as Kerberos KDCs support this value.

[<4> Section 2.4.1](#Appendix_A_Target_4): Only Windows Server 2012 and Windows Server 2012 R2 acting as Kerberos KDCs support this value for protocol transition (S4U2Self)-based service tickets

[<5> Section 2.4.2.4](#Appendix_A_Target_5): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2012 operating system, and Windows Server 2008 R2.

[<6> Section 2.4.2.4](#Appendix_A_Target_6): Not supported by Windows 2000.

[<7> Section 2.4.2.4](#Appendix_A_Target_7): Not supported by Windows 2000.

[<8> Section 2.4.2.4](#Appendix_A_Target_8): Not supported by Windows 2000.

[<9> Section 2.4.2.4](#Appendix_A_Target_9): Supported in Windows Server 2003 and Windows Server 2008. The DC adds this [SID](#Section_78eb90131c3a4970ad1f2b1dad588a25):

* When the user is a member of the forest.
* When the user is not a member of the forest and the TRUST\_ATTRIBUTE\_CROSS\_ORGANIZATION bit of the Trust Attribute ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.6.7.9) of the trusted domain object is not set.

[<10> Section 2.4.2.4](#Appendix_A_Target_10): The COMPOUNDED\_AUTHENTICATION SID is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

[<11> Section 2.4.2.4](#Appendix_A_Target_11): The CLAIMS\_VALID SID is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

[<12> Section 2.4.2.4](#Appendix_A_Target_12): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, or Windows Server 2012.

[<13> Section 2.4.2.4](#Appendix_A_Target_13): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, or Windows Server 2012 R2.

[<14> Section 2.4.2.4](#Appendix_A_Target_14): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, or Windows Server 2012 R2.

[<15> Section 2.4.2.4](#Appendix_A_Target_15): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista.

[<16> Section 2.4.2.4](#Appendix_A_Target_16): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista.

[<17> Section 2.4.2.4](#Appendix_A_Target_17): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT.

[<18> Section 2.4.2.4](#Appendix_A_Target_18): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<19> Section 2.4.2.4](#Appendix_A_Target_19): A built-in group that is created when a domain controller is added to the domain Not supported by Windows NT, Windows XP, and Windows 2000.

[<20> Section 2.4.2.4](#Appendix_A_Target_20): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<21> Section 2.4.2.4](#Appendix_A_Target_21): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<22> Section 2.4.2.4](#Appendix_A_Target_22): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<23> Section 2.4.2.4](#Appendix_A_Target_23): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<24> Section 2.4.2.4](#Appendix_A_Target_24): A new local group is created for Windows Server 2003 operating system with Service Pack 1 (SP1), Windows Server 2003 operating system with Service Pack 2 (SP2), Windows Server 2003 operating system with Service Pack 3 (SP3), Windows Server 2008, Windows Server 2008 R2 operating system, Windows Server 2012, Windows Server 2012 R2 operating system, Windows Server 2016, and Windows Server operating system.

[<25> Section 2.4.2.4](#Appendix_A_Target_25): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, and Windows 2000.

[<26> Section 2.4.2.4](#Appendix_A_Target_26): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, Windows 2000, and Windows Server 2003.

[<27> Section 2.4.2.4](#Appendix_A_Target_27): A built-in group that is created when a domain controller is added to the domain. Not supported by Windows NT, Windows XP, Windows 2000, and Windows Server 2003.

[<28> Section 2.4.2.4](#Appendix_A_Target_28): A built-in group that is created when a domain controller is added to the domain Not supported by Windows NT, Windows XP, Windows 2000, and Windows Server 2003.

[<29> Section 2.4.2.4](#Appendix_A_Target_29): The THIS\_ORGANIZATION\_CERTIFICATE SID is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<30> Section 2.4.2.4](#Appendix_A_Target_30): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, or Windows Server 2012.

[<31> Section 2.4.2.4](#Appendix_A_Target_31): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, or Windows Server 2012.

[<32> Section 2.4.2.4](#Appendix_A_Target_32): Supported in Windows Server 2003 and Windows Server 2008. When the TRUST\_ATTRIBUTE\_CROSS\_ORGANIZATION bit of the Trust Attribute ([MS-ADTS] section 6.1.6.7.9) of the trusted domain object is set:

* If the forest boundary is crossed, Windows domain controllers add this SID.
* If Windows domain controllers receive requests to authenticate to resources in their domain, they check the computer object to ensure that this SID is allowed. In Windows, by default this applies to NTLM (as specified in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) and [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e)), to Kerberos (as specified in [[MS-KILE]](%5bMS-KILE%5d.pdf#Section_2a32282edd484ad9a542609804b02cc9) and [MS-APDS]), and to TLS (as specified in [[MS-TLSP]](%5bMS-TLSP%5d.pdf#Section_58aba05b62b04cd1b88bdc8a24920346) and [[MS-SFU]](%5bMS-SFU%5d.pdf#Section_3bff58648135400ebdd933b552051d94)).

[<33> Section 2.4.2.4](#Appendix_A_Target_33): Not supported in Windows NT, Windows 2000, Windows XP, or Windows Server 2003.

[<34> Section 2.4.2.4](#Appendix_A_Target_34): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

[<35> Section 2.4.2.4](#Appendix_A_Target_35): Only Kerberos KDCs provide this SID, which is not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

[<36> Section 2.4.2.4](#Appendix_A_Target_36): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

[<37> Section 2.4.2.4](#Appendix_A_Target_37): Only Kerberos KDCs provide this SID for protocol transition (S4U2Self) based service tickets, which are not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

[<38> Section 2.4.2.4](#Appendix_A_Target_38): Only Kerberos KDCs provide this SID for tickets based on [[IETFDRAFT-PK-FRESH]](https://go.microsoft.com/fwlink/?LinkId=534982). FRESH\_PUBLIC\_KEY\_IDENTITY is not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

[<39> Section 2.4.2.4](#Appendix_A_Target_39): Only Kerberos KDCs provide this SID when key trust attributes are used for validation. KEY\_TRUST\_ IDENTITY is not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

[<40> Section 2.4.2.4](#Appendix_A_Target_40): Only Kerberos KDCs provide this SID when key trust attributes for MFA is true. KEY\_PROPERTY\_MFA is not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

[<41> Section 2.4.2.4](#Appendix_A_Target_41): Only Kerberos KDCs provide this SID when key trust attributes for attestation is true. KEY\_PROPERTY\_ATTESTATION is not supported in Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

[<42> Section 2.4.4.1](#Appendix_A_Target_42): Windows NT 4.0 operating system: Not supported.

[<43> Section 2.4.4.1](#Appendix_A_Target_43): Windows NT 4.0: Not supported.

[<44> Section 2.4.4.1](#Appendix_A_Target_44): Windows NT 4.0: Not supported.

[<45> Section 2.4.4.1](#Appendix_A_Target_45): Windows NT 4.0 and Windows 2000: Not supported.

[<46> Section 2.4.4.1](#Appendix_A_Target_46): Windows NT 4.0 and Windows 2000: Not supported.

[<47> Section 2.4.4.1](#Appendix_A_Target_47): Windows NT 4.0 and Windows 2000: Not supported.

[<48> Section 2.4.4.1](#Appendix_A_Target_48): Windows NT 4.0 and Windows 2000: Not supported.

[<49> Section 2.4.4.1](#Appendix_A_Target_49): Windows NT 4.0 and Windows 2000: Not supported.

[<50> Section 2.4.4.1](#Appendix_A_Target_50): Callback in this context relates to the local-only AuthzAccessCheck function, as described in [[MSDN-AuthzAccessCheck]](https://go.microsoft.com/fwlink/?LinkId=204597).

[<51> Section 2.4.4.1](#Appendix_A_Target_51): Windows NT 4.0: Not supported.

[<52> Section 2.4.4.13](#Appendix_A_Target_52): This construct is not supported by Windows NT, Windows 2000, Windows XP, or Windows Server 2003.

[<53> Section 2.4.4.17](#Appendix_A_Target_53): Conditional ACEs are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008.

[<54> Section 2.4.4.17.6](#Appendix_A_Target_54): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<55> Section 2.4.4.17.6](#Appendix_A_Target_55): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<56> Section 2.4.4.17.6](#Appendix_A_Target_56): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<57> Section 2.4.4.17.6](#Appendix_A_Target_57): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<58> Section 2.4.4.17.6](#Appendix_A_Target_58): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<59> Section 2.4.4.17.6](#Appendix_A_Target_59): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<60> Section 2.4.4.17.6](#Appendix_A_Target_60): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<61> Section 2.4.4.17.6](#Appendix_A_Target_61): The @Prefixed form is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<62> Section 2.4.4.17.6](#Appendix_A_Target_62): Windows implementations do not set this flag by default.

[<63> Section 2.4.4.17.6](#Appendix_A_Target_63): For Windows 7 and Windows Server 2008 R2, the LHS is an attribute name in simple form and RHS is a single literal value. Evaluates to TRUE if the set of values for the specified LHS includes a value identical to the specified literal; otherwise, FALSE.

[<64> Section 2.4.4.17.6](#Appendix_A_Target_64): For Windows 7 and Windows Server 2008 R2, the RHS is either a list of literals or a single literal value. Evaluates to TRUE if the LHS is a superset of the value of the specified RHS; otherwise, FALSE.

[<65> Section 2.4.4.17.6](#Appendix_A_Target_65): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<66> Section 2.4.4.17.6](#Appendix_A_Target_66): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<67> Section 2.4.4.17.7](#Appendix_A_Target_67): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<68> Section 2.4.5](#Appendix_A_Target_68): Not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

[<69> Section 2.4.6](#Appendix_A_Target_69): Windows typically presents the target fields in this order: Sacl, Dacl, OwnerSid, GroupSid.

[<70> Section 2.4.6](#Appendix_A_Target_70): Windows sets **Sbz1** to zero for Windows resources.

[<71> Section 2.4.6](#Appendix_A_Target_71): This field is intended only for use by the POSIX subsystem and is otherwise ignored by the Windows access control components.

[<72> Section 2.4.10.1](#Appendix_A_Target_72): These values are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<73> Section 2.4.10.1](#Appendix_A_Target_73): These values are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<74> Section 2.4.10.1](#Appendix_A_Target_74): This value is ignored by Windows when set on a security descriptor.

[<75> Section 2.4.10.2](#Appendix_A_Target_75): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008.

[<76> Section 2.5.1](#Appendix_A_Target_76): SDDL was introduced in Windows 2000.

[<77> Section 2.5.1.1](#Appendix_A_Target_77): GUIDs are not supported on Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<78> Section 2.5.1.1](#Appendix_A_Target_78): For the domain built-in ADMINISTRATOR (S-1-5-21-<domain>-500), Windows passes the actual SID, not the "LA" token. Reporting tools might convert this back to a token when examining the SDDL.

[<79> Section 2.5.1.1](#Appendix_A_Target_79): Not all conditional ACE types are supported in the SDDL. The conditional ACE types ACCESS\_ALLOWED\_CALLBACK\_ACE and ACCESS\_DENIED\_CALLBACK\_ACE are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008. The conditional ACE types ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE and SYSTEM\_AUDIT\_CALLBACK\_ACE are not supported in Windows 7 and Windows Server 2008 R2.

[<80> Section 2.5.1.1](#Appendix_A_Target_80): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<81> Section 2.5.1.1](#Appendix_A_Target_81): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<82> Section 2.5.1.1](#Appendix_A_Target_82): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<83> Section 2.5.1.1](#Appendix_A_Target_83): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<84> Section 2.5.1.1](#Appendix_A_Target_84): "Member\_of", "Not\_Member\_of", "Member\_of\_Any", "Not\_Member\_of\_Any", "Device\_Member\_of", "Device\_Member\_of\_Any", "Not\_Device\_Member\_of", and "Not\_Device\_Member\_of\_Any" are not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008. Only "Member\_of" is supported in Windows 7 and Windows Server 2008 R2.

[<85> Section 2.5.1.1](#Appendix_A_Target_85): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<86> Section 2.5.1.1](#Appendix_A_Target_86): Not\_Contains is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<87> Section 2.5.1.1](#Appendix_A_Target_87): Not\_Any is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<88> Section 2.5.1.1](#Appendix_A_Target_88): Use of the @ symbol in the simple form is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<89> Section 2.5.1.1](#Appendix_A_Target_89): Not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2.

[<90> Section 2.5.2](#Appendix_A_Target_90): For all Windows versions except Windows XP and Windows Server 2003, the policy is that **OwnerIndex** is always the same as **UserIndex**, except for members of the local Administrators group, in which case the **OwnerIndex** is set to the index for the SID representing the Administrators group. For Windows XP and Windows Server 2003, there is a policy that allows the **OwnerIndex** to be the **UserIndex** under all conditions.

[<91> Section 2.5.3.1.4](#Appendix_A_Target_91): An implementation-specific local recovery policy is a central access policy that allows the implementation itself, and the authorities that manage it, access to the resource being protected in disaster recovery scenarios. The Windows local recovery policy ensures administrators and the system have access to resources while Windows is booted in safe mode.

[<92> Section 2.5.3.3](#Appendix_A_Target_92): The Windows integrity mechanism extension is not supported in Windows NT, Windows 2000, Windows XP, or Windows Server 2003.

[<93> Section 2.5.3.4](#Appendix_A_Target_93): Assigning the owner and group fields in the security descriptor uses the following logic:

1. If the security descriptor that is supplied for the object by the caller includes an owner, it is assigned as the owner of the new object. Otherwise, if the DEFAULT\_OWNER\_FROM\_PARENT flag (see section [2.5.3.4.1](#Section_98267ad666db4a2c972eefb7d4603da1)) is set, the new object is assigned the same owner as the parent object. If this flag is not set, the default owner specified by the token (see section 2.5.3.4.1) is assigned.
2. If the security descriptor that is supplied for the object by the caller includes a group, it is assigned as the group of the new object. Otherwise, if the DEFAULT\_GROUP\_FROM\_PARENT flag (see section 2.5.3.4.1) is set, the new object is assigned the same primary group as the parent object. If this flag is not set, the default group specified by the token (see section 2.5.3.4.1) is assigned.

# Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

* A document revision that incorporates changes to interoperability requirements.
* A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

| Section | Description | Revision class |
| --- | --- | --- |
| [2.4.6](#Section_7d4dac059cef4563a058f108abecce1d) SECURITY\_DESCRIPTOR | 8233 : Reversed the order of the DT and SS control flags to match observed values. | Major |

# Index

A

[ACCESS\_ALLOWED\_ACE packet](#section_72e7c7eabc024c74a619818a16bf6adb) 55

[ACCESS\_ALLOWED\_CALLBACK\_ACE packet](#section_c9579cf40f4a44f19444422dfb10557a) 60

[ACCESS\_ALLOWED\_CALLBACK\_OBJECT\_ACE packet](#section_fe1838eaea344a5eb40eeb870f8322ae) 61

[ACCESS\_ALLOWED\_OBJECT\_ACE packet](#section_c79a383c2b3f4655abe7dcbb7ce0cfbe) 56

[ACCESS\_CONTROL\_ASSISTANCE\_OPS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ACCESS\_DENIED\_ACE packet](#section_b1e1321d58164513be67b65d8ae52fe8) 58

[ACCESS\_DENIED\_CALLBACK\_ACE packet](#section_35adad6bfda54cc1b1b59beda5b07d2e) 60

[ACCESS\_DENIED\_CALLBACK\_OBJECT\_ACE packet](#section_4652f21182d54b90bd5843bf3b0fc48d) 62

[ACCESS\_DENIED\_OBJECT\_ACE packet](#section_8720fcf3865c455797b10b3489a6c270) 58

[ACCOUNT\_OPERATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ACE\_HEADER packet](#section_628ebb1dc5094ea0a10f77ef97ca4586) 53

[ACE\_HEADER structure](#section_66fe5ecdf4e14a35b7de10e489a45a93) 55

[ACL packet](#section_20233ed8a6c64097aafadd545ed24428) 81

[ACL structure](#section_32d722570e7c4782bc2a405af4d5469d) 83

[ADMINISTRATOR](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ALIAS\_PREW2KCOMPACC](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ALL\_APP\_PACKAGES](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ANONYMOUS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Applicability](#section_54e14d592cfe49329764d92f1f598ade) 13

[AUTHENTICATED\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[AUTHENTICATION\_AUTHORITY\_ASSERTED\_IDENTITY](#section_81d92bbad22b4a8c908a554ab29148ab) 42

B

[BACKUP\_OPERATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[BATCH](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[BUILTIN\_ADMINISTRATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[BUILTIN\_GUESTS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[BUILTIN\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

C

[Capability negotiation](#section_60e81cefd79a40b8b98c368c9c39fc2b) 13

[CERT\_PUBLISHERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[CERTIFICATE\_SERVICE\_DCOM\_ACCESS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Change tracking](#section_e0e95308df3748aba5afcbe30beebd2e) 149

[CLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE structure](#section_9020a075c1af4b03930bba785743bcab) 90

[CLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1 structure](#section_21f2b5f0737645bbbc31eaa60841dbe9) 88

[CLAIMS\_VALID](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[CLONEABLE\_CONTROLLERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Common base types](#section_3caa4769b02f4ceea8578496f4395ec1) 14

[Common data structures](#section_ad05c0d31a4f479980d1ffc5299da73e) 28

[Common data types](#section_efda83146e414837829938ba0ee04b92) 16

[COMPOUNDED\_AUTHENTICATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[CONSOLE\_LOGON](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Constructed security types](#section_4bc165d6d3114f368bc267a5373f8cf2) 38

[CREATOR\_GROUP](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[CREATOR\_OWNER](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[CRYPTOGRAPHIC\_OPERATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

D

[Data types](#section_432cd7e762764c8287fc50bbcbd5ffa0) 14

[common base types](#section_3caa4769b02f4ceea8578496f4395ec1) 14

[common data structures](#section_ad05c0d31a4f479980d1ffc5299da73e) 28

[common data types](#section_efda83146e414837829938ba0ee04b92) 16

[constructed security types](#section_4bc165d6d3114f368bc267a5373f8cf2) 38

[security types - additional information](#section_62310a1cb0c8499f9253aff25c7d12ff) 91

[DIALUP](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DIGEST\_AUTHENTICATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DISTRIBUTED\_COM\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DOMAIN\_ADMINS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DOMAIN\_COMPUTERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DOMAIN\_DOMAIN\_CONTROLLERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DOMAIN\_GUESTS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[DOMAIN\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

E

[ENTERPRISE\_ADMINS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ENTERPRISE\_DOMAIN\_CONTROLLERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ENTERPRISE\_READONLY\_DOMAIN\_CONTROLLERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[EVENT\_DESCRIPTOR structure](#section_a6110d3628c14290b79e26aa95a0b1a0) 28

[EVENT\_HEADER structure](#section_fa4f783606ee4ab68688386a5a85f8c5) 29

[EVENT\_LOG\_READERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[EVERYONE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Examples - structure](#section_386da4d11fd2482786615c4f9e21264a) 136

F

[Fields - vendor-extensible](#section_a66a31be16c94d89a865dc6055f8ba7b) 13

[FILETIME structure](#section_2c57429bfdd4488fb5fc9e4cf020fcdf) 31

G

[Glossary](#section_a66edeb152a04d64a93b2f5c833d7d92) 8

[GROUP\_POLICY\_CREATOR\_OWNERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[GROUP\_SERVER](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[GUEST](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[GUID packet](#section_001eec5a7f8b42939e21ca349392db40) 32

[GUID structure](#section_49e490b8f97245d6a3a499f924998d97) 31

H

[HYPER\_V\_ADMINS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

I

[IIS\_IUSRS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Implementer - security considerations](#section_298b510f786949099fa43fa6c81f2c05) 137

[INCOMING\_FOREST\_TRUST\_BUILDERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Informative references](#section_eaff25bc6c094428a44dcb0d1b4c64b7) 12

[INTERACTIVE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Introduction](#section_48a7a50982bf40f4a2ea30a8b549761a) 8

[IUSR](#section_81d92bbad22b4a8c908a554ab29148ab) 42

L

[LARGE\_INTEGER structure](#section_e904b1baf7744203ba1b66485165ab1a) 32

[LOCAL](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[LOCAL\_ACCOUNT](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[LOCAL\_ACCOUNT\_AND\_MEMBER\_OF\_ADMINISTRATORS\_GROUP](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[LOCAL\_SERVICE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[LOCAL\_SYSTEM](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Localization](#section_60e81cefd79a40b8b98c368c9c39fc2b) 13

[LOGON\_ID](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[LPFILETIME](#section_2c57429bfdd4488fb5fc9e4cf020fcdf) 31

[LPSERVER\_INFO\_100](#section_007c654b7d7849d49f4d0da7c1889727) 34

[LPSERVER\_INFO\_101](#section_39c502dd022b4a68936789fd76a23bc3) 35

[LUID structure](#section_48cbee2a079045f28269931d7083b2c3) 33

M

[MANDATORY\_INFORMATION structure](#section_6e6e65f4a64b4934b16e11490ae27f03) 88

[ML\_HIGH](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_LOW](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_MEDIUM](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_MEDIUM\_PLUS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_PROTECTED\_PROCESS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_SYSTEM](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[ML\_UNTRUSTED](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[MULTI\_SZ structure](#section_fd7b2d81b1d7414fa3dfc66fabc578db) 33

N

[NETWORK](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[NETWORK\_CONFIGURATION\_OPS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[NETWORK\_SERVICE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Normative references](#section_162f1e8c49874ad5a2f2368f808d1528) 11

[NT\_AUTHORITY](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[NT\_SERVICE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[NTLM\_AUTHENTICATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[NULL](#section_81d92bbad22b4a8c908a554ab29148ab) 42

O

[OBJECT\_TYPE\_LIST structure](#section_6f04f1f2d0704f70aae75f98ed63e1ba) 33

[OTHER\_ORGANIZATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Overview (synopsis)](#section_32dfc66cd7374e1bb67f6cf3a5bdefc7) 12

[OWNER\_RIGHTS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[OWNER\_SERVER](#section_81d92bbad22b4a8c908a554ab29148ab) 42

P

[PACE\_HEADER](#section_66fe5ecdf4e14a35b7de10e489a45a93) 55

[PACL](#section_32d722570e7c4782bc2a405af4d5469d) 83

[PCEVENT\_DESCRIPTOR](#section_a6110d3628c14290b79e26aa95a0b1a0) 28

[PCLAIM\_SECURITY\_ATTRIBUTE\_OCTET\_STRING\_RELATIVE](#section_9020a075c1af4b03930bba785743bcab) 90

[PCLAIM\_SECURITY\_ATTRIBUTE\_RELATIVE\_V1](#section_21f2b5f0737645bbbc31eaa60841dbe9) 88

[PERFLOG\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PERFMON\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PEVENT\_DESCRIPTOR](#section_a6110d3628c14290b79e26aa95a0b1a0) 28

[PEVENT\_HEADER](#section_fa4f783606ee4ab68688386a5a85f8c5) 29

[PFILETIME](#section_2c57429bfdd4488fb5fc9e4cf020fcdf) 31

[PGUID](#section_49e490b8f97245d6a3a499f924998d97) 31

[PLARGE\_INTEGER](#section_e904b1baf7744203ba1b66485165ab1a) 32

[PLUID](#section_48cbee2a079045f28269931d7083b2c3) 33

[PMANDATORY\_INFORMATION](#section_6e6e65f4a64b4934b16e11490ae27f03) 88

[POBJECT\_TYPE\_LIST](#section_6f04f1f2d0704f70aae75f98ed63e1ba) 33

[POWER\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PRINCIPAL\_SELF](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PRINTER\_OPERATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Product behavior](#section_11e1608c61694fbc9c33373fc9b224f4) 143

[PROTECTED\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PROXY](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[PRPC\_SID](#section_5cb97814a1c24215b7dc76d1f4bfad01) 41

[PRPC\_UNICODE\_STRING](#section_94a16bb6c6104cb98db626f15f560061) 34

[PSECURITY\_DESCRIPTOR](#section_f1e181673ddf48ada3d4b7e832f96b95) 86

[PSERVER\_INFO\_100](#section_007c654b7d7849d49f4d0da7c1889727) 34

[PSERVER\_INFO\_101](#section_39c502dd022b4a68936789fd76a23bc3) 35

[PSID](#section_5cb97814a1c24215b7dc76d1f4bfad01) 41

[PSYSTEM\_MANDATORY\_LABEL\_ACE](#section_59742407d7564aa68c31f3da27fff893) 68

[PSYSTEMTIME](#section_2fefe8ddab484e33a7d57171455a9289) 38

[PTOKEN\_MANDATORY\_POLICY](#section_de8373ec206f4dc8b3fec638fed7b282) 87

[PUINT128](#section_3b5c1a61ece44dce9c9fc15388ba9032) 38

[PULARGE\_INTEGER](#section_d37e0ce7a3584c07a5c459c8b5da8b08) 38

R

[RAS\_SERVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[RDS\_ENDPOINT\_SERVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[RDS\_MANAGEMENT\_SERVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[RDS\_REMOTE\_ACCESS\_SERVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[READONLY\_DOMAIN\_CONTROLLERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

References

[informative](#section_eaff25bc6c094428a44dcb0d1b4c64b7) 12

[normative](#section_162f1e8c49874ad5a2f2368f808d1528) 11

[Relationship to other protocols](#section_5b521fdb1a71422aa2565bdbd4ed06cf) 13

[Relationship to protocols and other structures](#section_5b521fdb1a71422aa2565bdbd4ed06cf) 13

[REMOTE\_DESKTOP](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[REMOTE\_INTERACTIVE\_LOGON](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[REMOTE\_MANAGEMENT\_USERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[REPLICATOR](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[RESTRICTED\_CODE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[RPC\_SID structure](#section_5cb97814a1c24215b7dc76d1f4bfad01) 41

[RPC\_SID\_IDENTIFIER\_AUTHORITY structure](#section_d7e6e5a5437c41e58ba1bdfd43e96cbc) 39

[RPC\_UNICODE\_STRING structure](#section_94a16bb6c6104cb98db626f15f560061) 34

S

[SCHANNEL\_AUTHENTICATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[SCHEMA\_ADMINISTRATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[Security - implementer considerations](#section_298b510f786949099fa43fa6c81f2c05) 137

[Security considerations](#section_298b510f786949099fa43fa6c81f2c05) 137

[Security types - data types](#section_62310a1cb0c8499f9253aff25c7d12ff) 91

[SECURITY\_DESCRIPTOR packet](#section_7d4dac059cef4563a058f108abecce1d) 83

[SECURITY\_DESCRIPTOR structure](#section_f1e181673ddf48ada3d4b7e832f96b95) 86

[SERVER\_INFO\_100 structure](#section_007c654b7d7849d49f4d0da7c1889727) 34

[SERVER\_INFO\_101 structure](#section_39c502dd022b4a68936789fd76a23bc3) 35

[SERVER\_OPERATORS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[SERVICE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[SERVICE\_ASSERTED\_IDENTITY](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[SID packet](#section_f992ad600fe44b879fedbeb478836861) 41

[SID\_IDENTIFIER\_AUTHORITY packet](#section_c6ce42753d904890ab3a514745e4637e) 38

[Structure examples](#section_386da4d11fd2482786615c4f9e21264a) 136

[SYSTEM\_AUDIT\_ACE packet](#section_9431fd0f5b9a47f0b3f03015e2d0d4f9) 64

[SYSTEM\_AUDIT\_CALLBACK\_ACE packet](#section_bd6b6fd84bef427e9a43b9b46457e934) 66

SYSTEM\_AUDIT\_CALLBACK\_OBJECT\_ACE packet ([section 2.4.4.11](#section_c8da72ae6b544a0585f4e2594936d3d5) 65, [section 2.4.4.14](#section_949b02e7f55d4c26969f52a009597469) 68)

[SYSTEM\_MANDATORY\_LABEL\_ACE packet](#section_25fa65656cb046aba30a016b32c4939a) 67

[SYSTEM\_MANDATORY\_LABEL\_ACE structure](#section_59742407d7564aa68c31f3da27fff893) 68

[SYSTEM\_RESOURCE\_ATTRIBUTE\_ACE packet](#section_352944c74fb6498880360a25dcedc730) 70

[SYSTEM\_SCOPED\_POLICY\_ID\_ACE packet](#section_aa0c0f624b4c44f09718c266a6accd9f) 71

[SYSTEMTIME structure](#section_2fefe8ddab484e33a7d57171455a9289) 38

T

[TERMINAL\_SERVER\_LICENSE\_SERVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[TERMINAL\_SERVER\_USER](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[THIS\_ORGANIZATION](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[THIS\_ORGANIZATION\_CERTIFICATE](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[TOKEN\_MANDATORY\_POLICY structure](#section_de8373ec206f4dc8b3fec638fed7b282) 87

[Tracking changes](#section_e0e95308df3748aba5afcbe30beebd2e) 149

U

[UINT128 structure](#section_3b5c1a61ece44dce9c9fc15388ba9032) 38

[ULARGE\_INTEGER structure](#section_d37e0ce7a3584c07a5c459c8b5da8b08) 38

[USER\_MODE\_DRIVERS](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[UUID](#section_49e490b8f97245d6a3a499f924998d97) 31

V

[Vendor-extensible fields](#section_a66a31be16c94d89a865dc6055f8ba7b) 13

[Versioning](#section_60e81cefd79a40b8b98c368c9c39fc2b) 13

W

[WINDOWS\_AUTHORIZATION\_ACCESS\_GROUP](#section_81d92bbad22b4a8c908a554ab29148ab) 42

[WRITE\_RESTRICTED\_CODE](#section_81d92bbad22b4a8c908a554ab29148ab) 42